#5

Docket No. 204258US6

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Naomi GO, et al
GAU:
SERIAL NO: NEW APPLICATION
EXAMINER:
FILED: HEREWITH
FOR: INFORMATION PROVIDING APPARATUS AND METHOD, INFORMATION PROCESSING APPARATUS AND METHOD, AND PROGRAM STORAGE MEDIUM

REQUEST FOR PRIORITY

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

☐ Full benefit of the filing date of U.S. Application Serial Number, filed, is claimed pursuant to the provisions of **35 U.S.C. §120**.

☐ Full benefit of the filing date of U.S. Provisional Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §119(e)**.

■ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY	APPLICATION NUMBER	MONTH/DAY/YEAR
JAPAN	2000-070461	March 14, 2000

Certified copies of the corresponding Convention Application(s)

■ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

☐ were filed in prior application Serial No. filed

☐ were submitted to the International Bureau in PCT Application Number .
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

(B) Application Serial No.(s)

☐ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Gregory J. Maier
Registration No. 25,599
C. Irvin McClelland
Registration Number 21,124

22850
Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 10/98)

JO P03650500

日　本　国　特　許　庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　３月１４日

出願番号
Application Number: 特願２０００－０７０４６１

出願人
Applicant (s): ソニー株式会社

２０００年１２月２２日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３１０６１４６

【書類名】　特許願
【整理番号】　0000130306
【提出日】　平成12年 3月14日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 12/16
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　郷　直美
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　栗原　章
【特許出願人】
　【識別番号】　000002185
　【氏名又は名称】　ソニー株式会社
　【代表者】　出井　伸之
【代理人】
　【識別番号】　100082131
　【弁理士】
　【氏名又は名称】　稲本　義雄
　【電話番号】　03-3369-6479
【手数料の表示】
　【予納台帳番号】　032089
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1

【包括委任状番号】　9708842

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　情報提供装置および方法、情報処理装置および方法、並びにプログラム格納媒体

【特許請求の範囲】

【請求項１】　第１の情報処理装置を認証する第１の認証手段と、

第２の情報処理装置または第３の情報処理装置を認証する第２の認証手段と、

前記第１の情報処理装置からの、コンテンツおよび鍵の送信要求、並びに前記第２の情報処理装置を特定するデータまたは前記第３の情報処理装置を特定するデータの受信を制御する受信制御手段と、

前記第２の情報処理装置を特定する前記データを受信した場合、前記第２の情報処理装置に対応した手順で、前記第２の情報処理装置に前記コンテンツおよび前記鍵の送信要求を送信するとともに、前記第２の情報処理装置から前記コンテンツおよび前記鍵を受信し、前記第３の情報処理装置を特定する前記データを受信した場合、前記第３の情報処理装置に対応した手順で、前記第３の情報処理装置に前記コンテンツおよび前記鍵の送信要求を送信するとともに、前記第３の情報処理装置から前記コンテンツおよび前記鍵を受信するように通信を制御する通信制御手段と、

前記第１の情報処理装置への前記コンテンツおよび前記鍵の送信を制御する送信制御手段と

を含むことを特徴とする情報提供装置。

【請求項２】　前記コンテンツの符号化方式および暗号化方式のうちの少なくとも一方を、所定の符号化方式または暗号化方式に変換する変換手段

を更に含むことを特徴とする請求項１に記載の情報提供装置。

【請求項３】　第１の情報処理装置を認証する第１の認証ステップと、

第２の情報処理装置または第３の情報処理装置を認証する第２の認証ステップと、

前記第１の情報処理装置からの、コンテンツおよび鍵の送信要求、並びに前記第２の情報処理装置を特定するデータまたは前記第３の情報処理装置を特定するデータの受信を制御する受信制御ステップと、

前記第２の情報処理装置を特定する前記データを受信した場合、前記第２の情報処理装置に対応した手順で、前記第２の情報処理装置に前記コンテンツおよび前記鍵の送信要求を送信するとともに、前記第２の情報処理装置から前記コンテンツおよび前記鍵を受信し、前記第３の情報処理装置を特定する前記データを受信した場合、前記第３の情報処理装置に対応した手順で、前記第３の情報処理装置に前記コンテンツおよび前記鍵の送信要求を送信するとともに、前記第３の情報処理装置から前記コンテンツおよび前記鍵を受信するように通信を制御する通信制御ステップと、

前記第１の情報処理装置への前記コンテンツおよび前記鍵の送信を制御する送信制御ステップと

を含むことを特徴とする情報提供方法。

【請求項４】　第１の情報処理装置を認証する第１の認証ステップと、

第２の情報処理装置または第３の情報処理装置を認証する第２の認証ステップと、

前記第１の情報処理装置からの、コンテンツおよび鍵の送信要求、並びに前記第２の情報処理装置を特定するデータまたは前記第３の情報処理装置を特定するデータの受信を制御する受信制御ステップと、

前記第２の情報処理装置を特定する前記データを受信した場合、前記第２の情報処理装置に対応した手順で、前記第２の情報処理装置に前記コンテンツおよび前記鍵の送信要求を送信するとともに、前記第２の情報処理装置から前記コンテンツおよび前記鍵を受信し、前記第３の情報処理装置を特定する前記データを受信した場合、前記第３の情報処理装置に対応した手順で、前記第３の情報処理装置に前記コンテンツおよび前記鍵の送信要求を送信するとともに、前記第３の情報処理装置から前記コンテンツおよび前記鍵を受信するように通信を制御する通信制御ステップと、

前記第１の情報処理装置への前記コンテンツおよび前記鍵の送信を制御する送信制御ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが格納されているプログラム格納媒体。

【請求項５】　第１の情報提供装置を認証する認証手段と、

前記第１の情報提供装置への、コンテンツおよび鍵の送信要求、並びに前記コンテンツおよび前記鍵を提供する第２の情報提供装置を特定するデータ、および前記コンテンツおよび前記鍵を提供する第３の情報提供装置を特定するデータのいずれかの送信を制御する送信制御手段と、

前記第２の情報提供装置または前記第３の情報提供装置から前記第１の情報提供装置が提供を受け、送信した前記コンテンツおよび前記鍵の受信を制御する受信制御手段と

を含むことを特徴とする情報処理装置。

【請求項６】　第１の情報提供装置を認証する認証ステップと、

前記第１の情報提供装置への、コンテンツおよび鍵の送信要求、並びに前記コンテンツおよび前記鍵を提供する第２の情報提供装置を特定するデータ、および前記コンテンツおよび前記鍵を提供する第３の情報提供装置を特定するデータのいずれかの送信を制御する送信制御ステップと、

前記第２の情報提供装置または前記第３の情報提供装置から前記第１の情報提供装置が提供を受け、送信した前記コンテンツおよび前記鍵の受信を制御する受信制御ステップと

を含むことを特徴とする情報処理方法。

【請求項７】　第１の情報提供装置を認証する認証ステップと、

前記第１の情報提供装置への、コンテンツおよび鍵の送信要求、並びに前記コンテンツおよび前記鍵を提供する第２の情報提供装置を特定するデータ、および前記コンテンツおよび前記鍵を提供する第３の情報提供装置を特定するデータのいずれかの送信を制御する送信制御ステップと、

前記第２の情報提供装置または前記第３の情報提供装置から前記第１の情報提供装置が提供を受け、送信した前記コンテンツおよび前記鍵の受信を制御する受信制御ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが格納されているプログラム格納媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報提供装置および方法、情報処理装置および方法、並びにプログラム格納媒体に関し、特に、コンテンツおよびコンテンツを復号する鍵を提供するか、または暗号化されているコンテンツを利用する情報提供装置および方法、情報処理装置および方法、並びにプログラム格納媒体に関する。

【０００２】

【従来の技術】

図１は、従来のデジタルデータ伝送システムの構成を示す図である。パーソナルコンピュータ１は、ローカルエリアネットワークまたはインターネットなどから構成される通信ネットワーク４に接続されている。パーソナルコンピュータ１は、コンテンツサーバ２２－１若しくは２２－２から受信した、またはCD（Compact Disc）から読み取った楽音のデータ（以下、コンテンツと称する）を、所定の圧縮の方式（例えば、ATRAC3（商標））に変換するとともにDES（Data Encryption Standard）などの暗号化方式で暗号化して記録する。

【０００３】

パーソナルコンピュータ１は、暗号化して記録しているコンテンツに対応して、コンテンツの利用条件を示す利用条件のデータを記録する。

【０００４】

利用条件のデータは、例えば、その利用条件のデータに対応するコンテンツを同時に利用することができるポータブルデバイス（Portable Device（PDとも称する））の台数（後述する、いわゆるチェックアウトできるPDの台数）を示す。利用条件のデータに示される数だけコンテンツをチェックアウトしたときでも、パーソナルコンピュータ１は、そのコンテンツを再生できる。

【０００５】

パーソナルコンピュータ１の表示操作指示プログラム１１は、パーソナルコンピュータ１が記録しているコンテンツに関連するデータ（例えば、曲名、または利用条件など）を表示させるとともに、チェックアウトの指示などを入力して、ＳＤＭＩ（Secure Digital Music Initiative）の規格に準拠したソフトウェア

モジュールであるＬＣＭ（Licensed Compliant Module）１２にその指示に対応したチェックアウトなどの処理を実行させる。

【０００６】

パーソナルコンピュータ１のＬＣＭ１２は、コンテンツの不正な２次利用による著作権の侵害の防止を目的として、個々のコンテンツに対して著作権者が指定する利用条件でのみコンテンツを利用できるように制御を行うモジュール群から構成される。利用条件には、コンテンツの再生条件、コピー条件、移動条件、または蓄積条件などが含まれる。

【０００７】

ＬＣＭ１２は、パーソナルコンピュータ１に接続された機器が正当であるかの認証を行い、安全な方法でコンテンツの移動の処理などを実行する。コンテンツの移動の処理などに伴い、ＬＣＭ１２は、必要な鍵を生成して、鍵を管理し、コンテンツを暗号化し、または接続されている機器との通信を制御する。

【０００８】

また、ＬＣＭ１２は、装着されているポータブルメディア３の正当性をチェックして、サーバ５が指定した利用条件をコンテンツ（暗号化されている）に付加して、コンテンツを記録させる。

【０００９】

パーソナルコンピュータ１のＬＣＭ１２は、暗号化して記録しているコンテンツを、コンテンツに関連するデータ（例えば、曲名、または利用条件など）と共に、接続されているポータブルデバイス２に供給するとともに、ポータブルデバイス２に供給したことに対応して、供給したコンテンツに対応する利用条件のデータを更新する（以下、チェックアウトと称する）。より詳細には、チェックアウトしたとき、パーソナルコンピュータ１が記録している、そのコンテンツに対応する利用条件のデータのチェックアウトできる回数は、１減らされる。チェックアウトできる回数が０のとき、対応するコンテンツは、チェックアウトすることができない。

【００１０】

ポータブルデバイス２は、パーソナルコンピュータ１から供給されたコンテン

ツ（すなわち、チェックアウトされたコンテンツ）を、コンテンツに関連するデータ（例えば、曲名、または利用条件など）と共に、装着されているポータブルメディア３に記憶させる。

【００１１】

ポータブルメディア３は、フラッシュメモリなどの記憶媒体をその内部に有し、ポータブルデバイス２に着脱可能に構成されている。

【００１２】

ポータブルデバイス２は、コンテンツに関連する利用条件のデータに基づいて、装着されているポータブルメディア３に記憶されているコンテンツを再生し、図示せぬヘッドフォンなどに出力する。

【００１３】

例えば、コンテンツに関連する利用条件のデータとして記憶されている、再生制限としての再生回数を超えて再生しようとしたとき、ポータブルデバイス２は、対応するコンテンツの再生を停止する。

【００１４】

使用者は、コンテンツを記憶したポータブルデバイス２をパーソナルコンピュータ１から取り外して、持ち歩き、ポータブルメディア３に記憶されているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

【００１５】

ポータブルデバイス２がUSBケーブル等を介してパーソナルコンピュータ１に接続されたとき、ポータブルデバイス２とパーソナルコンピュータ１とは、相互認証の処理を実行する。この相互認証の処理は、チャレンジレスポンス方式の認証の処理である。チャレンジレスポンス方式とは、パーソナルコンピュータ１が生成するある値（チャレンジ）に対して、ポータブルデバイス２がパーソナルコンピュータ１と共有している秘密鍵を使用して生成した値（レスポンス）で応答する方式である。

【００１６】

サーバ５－１は、所定の方式で圧縮符号化され、暗号化されたコンテンツを蓄

積して、パーソナルコンピュータ１からの要求に対応して蓄積しているコンテンツを配信する。サーバ５－１は、鍵サーバ２１－１、コンテンツサーバ２２－１、およびショップサーバ２３－１の機能を有する。

【００１７】

鍵サーバ２１－１は、コンテンツサーバ２２－１がパーソナルコンピュータ１に供給したコンテンツを復号するためのコンテンツ鍵を蓄積し、パーソナルコンピュータ１の要求に対応して、コンテンツ鍵をパーソナルコンピュータ１に供給する。コンテンツ鍵の供給の前に、鍵サーバ２１－１とパーソナルコンピュータ１とは、相互認証の処理を実行して、鍵サーバ２１－１は、その相互認証の処理により共有された一時鍵でコンテンツ鍵を暗号化して、パーソナルコンピュータ１に送信する。パーソナルコンピュータ１は、受信したコンテンツ鍵を共有している一時鍵で復号する。

【００１８】

コンテンツサーバ２２－１は、パーソナルコンピュータ１の要求に対応して、通信ネットワーク４を介して、パーソナルコンピュータ１に、コンテンツに対応する利用条件と共にコンテンツ（暗号化されている）を供給する。

【００１９】

ショップサーバ２３－１は、コンテンツサーバ２２－１が供給するコンテンツに関連するデジタルデータ（コンテンツの曲名、価格などを含むコンテンツの一覧などを含む）をパーソナルコンピュータ１に提供するとともに、パーソナルコンピュータ１からのコンテンツの購入の申し込みに対応して、そのコンテンツを供給するコンテンツサーバ２２－１のＵＲＬ（Uniform Resource Locator）、およびそのコンテンツを復号するコンテンツ鍵を供給する鍵サーバ２１－１のＵＲＬなどをパーソナルコンピュータ１に供給する。

【００２０】

サーバ５－２は、所定の方式で圧縮符号化され、暗号化されたコンテンツを蓄積して、パーソナルコンピュータ１からの要求に対応して蓄積しているコンテンツを配信する。サーバ５－２は、鍵サーバ２１－２、コンテンツサーバ２２－２、およびショップサーバ２３－２の機能を有する。

【００２１】

鍵サーバ２１－２は、コンテンツサーバ２２－２がパーソナルコンピュータ１に供給したコンテンツを復号するためのコンテンツ鍵を蓄積し、パーソナルコンピュータ１の要求に対応して、コンテンツ鍵をパーソナルコンピュータ１に供給する。コンテンツ鍵の供給の前に、鍵サーバ２１－２とパーソナルコンピュータ１とは、相互認証の処理を実行して、鍵サーバ２１－２は、その相互認証の処理により共有された一時鍵でコンテンツ鍵を暗号化して、パーソナルコンピュータ１に送信する。パーソナルコンピュータ１は、受信したコンテンツ鍵を共有している一時鍵で復号する。

【００２２】

コンテンツサーバ２２－２は、パーソナルコンピュータ１の要求に対応して、通信ネットワーク４を介して、パーソナルコンピュータ１に、コンテンツに対応する利用条件と共にコンテンツ（暗号化されている）を供給する。

【００２３】

ショップサーバ２３－２は、コンテンツサーバ２２－２が供給するコンテンツに関連するデジタルデータ（コンテンツの曲名、価格などを含むコンテンツの一覧などを含む）をパーソナルコンピュータ１に提供するとともに、パーソナルコンピュータ１からのコンテンツの購入の申し込みに対応して、そのコンテンツを供給するコンテンツサーバ２２－２のＵＲＬ、およびそのコンテンツを復号するコンテンツ鍵を供給する鍵サーバ２１－２のＵＲＬなどをパーソナルコンピュータ１に供給する。

【００２４】

以下、サーバ５－１およびサーバ５－２を個々に区別する必要がないとき、単に、サーバ５と称する。以下、鍵サーバ２１－１および鍵サーバ２１－２を個々に区別する必要がないとき、単に、鍵サーバ２１と称する。以下、コンテンツサーバ２２－１およびコンテンツサーバ２２－２を個々に区別する必要がないとき、単に、コンテンツサーバ２２と称する。以下、ショップサーバ２３－１およびショップサーバ２３－２を個々に区別する必要がないとき、単に、ショップサーバ２３と称する。

【００２５】

次に、図２を参照して、従来のデジタルデータ伝送システムの機能の構成について説明する。パーソナルコンピュータ１は、表示操作指示プログラム１１およびＬＣＭ１２に加えて、ＩＰ（Internet Protocol）通信プログラム１３、ＩＳＰ（Internet Service Provider）接続プログラム１４、およびＰＨＳ（Personal Handyphone System）／ＩＭＴ（International Mobile Telecommunication System）通信プログラム１５を実行する。

【００２６】

ＰＨＳ／ＩＭＴ通信プログラム１５は、公衆回線網３１を介して通信を行うためのプログラムである。ＩＳＰ接続プログラム１４は、ＩＳＰ３２と接続するためのプログラムである。ＩＰ通信プログラム１３は、ＨＴＴＰ（Hypertext Transport Protocol）７４およびＷａｐ（Wireless Access Protocol）７５などの手続を包含し、通信ネットワーク４を介して、鍵サーバ２１、コンテンツサーバ２２、またはショップサーバ２３と通信するためのプログラムである。

【００２７】

ＬＣＭ１２は、ライセンス管理プログラム５１、ダウンロードプログラム５２－１、ダウンロードプログラム５２－２、およびフォーマット管理プログラム５３から構成されている。

【００２８】

ライセンス管理プログラム５１は、コンテンツの利用条件に基づいたコンテンツの利用を管理するためのプログラムであり、利用条件管理プログラム６１、CDリッピングプログラム６２、およびPD認証プログラム６３から構成されている。

【００２９】

利用条件管理プログラム６１は、コンテンツの利用条件に基づいて、パーソナルコンピュータ１が記録しているコンテンツのチェックアウトなどを許可するか、または禁止するかなどの管理を実行するとともに、コンテンツのチェックアウトなどに対応して利用条件のデータを更新する。CDリッピングプログラム６２は、パーソナルコンピュータ１に装着されたCDからコンテンツを読み出すとともに、読み出したコンテンツに対応する利用条件を生成する。

【００３０】

PD認証プログラム６３は、パーソナルコンピュータ１に装着されているポータブルデバイス２を認証する。

【００３１】

ダウンロードプログラム５２－１は、サーバ５－１からコンテンツおよびコンテンツ鍵をダウンロードするためのプログラムであり、鍵管理プログラム６４、コンテンツ管理プログラム６５、鍵情報受信プログラム６６、およびコンテンツ情報受信プログラム６７から構成されている。

【００３２】

鍵管理プログラム６４は、鍵サーバ２１－１の認証の処理を実行して、鍵サーバ２１－１からコンテンツ鍵を受信して、コンテンツに対応させてコンテンツ鍵を管理する。鍵管理プログラム６４は、サーバ認証プログラム７１および受信プログラム７２から構成される。

【００３３】

サーバ認証プログラム７１は、後述する処理により、鍵サーバ２１－１を認証する。受信プログラム７２は、通信ネットワーク４を介して、鍵サーバ２１－１からコンテンツ鍵を受信する。

【００３４】

コンテンツ管理プログラム６５は、通信ネットワーク４を介して、コンテンツサーバ２２－１からコンテンツの利用条件のデータとともにコンテンツを受信して、コンテンツの利用条件のデータとともにコンテンツを記録する。コンテンツ管理プログラム６５の受信プログラム７３は、コンテンツサーバ２２－１からコンテンツの利用条件のデータおよびコンテンツを受信する。

【００３５】

鍵情報受信プログラム６６は、ショップサーバ２３－１から、所望のコンテンツに対応するコンテンツ鍵を供給する鍵サーバ２１－１を特定するＵＲＬを受信する。コンテンツ情報受信プログラム６７は、ショップサーバ２３－１から、使用者が所望するコンテンツを特定するコンテンツＩＤ、およびそのコンテンツを供給するコンテンツサーバ２２－１を特定するＵＲＬを受信する。

【００３６】

ダウンロードプログラム５２－２は、サーバ５－２からコンテンツおよびコンテンツ鍵をダウンロードするためのプログラムであり、ダウンロードプログラム５２－１と同様の構成を有するので、その説明は省略する。

【００３７】

フォーマット管理プログラム５３は、コンテンツサーバ２２－１または２２－２からダウンロードしたコンテンツの符号化方式および暗号化方式をそれぞれ所定の方式に変換するとともに、CDから読み出したコンテンツを所定の方式で符号化して暗号化する。フォーマット管理プログラム５３は、システム識別プログラム６８およびフォーマット変換プログラム６９から構成されている。

【００３８】

システム識別プログラム６８は、コンテンツのダウンロード先が、サーバ５－１であるか、サーバ５－２であるかのいずれかを識別するためのプログラムである。フォーマット変換プログラム６９は、コンテンツの符号化方式および暗号化方式を変換する。

【００３９】

ポータブルデバイス２は、ライセンス管理プログラム８１、鍵管理プログラム８２、およびコンテンツ管理プログラム８３を実行する。

【００４０】

ライセンス管理プログラム８１は、コンテンツに対応する利用条件を基に、コンテンツの再生の回数などを管理する利用条件管理プログラム９１、パーソナルコンピュータ１を認証するPC認証プログラム９２、およびポータブルメディア３を認証するPM認証プログラム９３から構成される。

【００４１】

鍵管理プログラム８２は、パーソナルコンピュータ１から供給されたコンテンツ鍵を、ポータブルメディア３が予め記憶している保存用鍵で暗号化させ、ポータブルメディア３に記憶させて管理する。

【００４２】

コンテンツ管理プログラム８３は、パーソナルコンピュータ１から供給された

コンテンツを、ポータブルメディア３に記憶させて管理する。

【００４３】

ポータブルメディア３は、ライセンス管理プログラム１０１、鍵管理プログラム１０２、およびコンテンツ管理プログラム１０３を実行する。

【００４４】

ライセンス管理プログラム１０１は、ポータブルデバイス２を認証するPD認証プログラム１１１を有し、コンテンツに対応する利用条件のデータを記憶して、利用条件のデータに基づいて、コンテンツの読み出し等を制御する。鍵管理プログラム１０２は、ポータブルデバイス２から供給されたコンテンツ鍵を、予め記憶している保存用鍵で暗号化して記憶し、管理する。コンテンツ管理プログラム１０３は、ポータブルデバイス２から供給されたコンテンツを記憶して、管理する。

【００４５】

ショップサーバ２３－１は、鍵情報送信プログラム１２１、コンテンツ情報送信プログラム１２２、閲覧プログラム１２３、およびＩＰ通信プログラム１２４を実行する。

【００４６】

鍵情報送信プログラム１２１は、通信ネットワーク４を介して、パーソナルコンピュータ１に、パーソナルコンピュータ１の使用者が所望するコンテンツに対応するコンテンツ鍵を供給する鍵サーバ２１－１のＵＲＬを送信する。

【００４７】

コンテンツ情報送信プログラム１２２は、通信ネットワーク４を介して、パーソナルコンピュータ１に、パーソナルコンピュータ１の使用者が所望するコンテンツを供給するコンテンツサーバ２２－１のＵＲＬを送信する。

【００４８】

閲覧プログラム１２３は、コンテンツをパーソナルコンピュータ１の使用者に視聴させる視聴プログラム１３１、およびパーソナルコンピュータ１の使用者が所望のコンテンツを検索する検索プログラム１３２から構成されている。

【００４９】

ＩＰ通信プログラム１２４は、ＨＴＴＰ１３３およびＷａｐ１３４などの手続を包含し、通信ネットワーク４を介して、パーソナルコンピュータ１と通信するためのプログラムである。

【００５０】

鍵サーバ２１－１は、認証プログラム１５１、鍵配信プログラム１５２、鍵保存プログラム１５３、鍵生成プログラム１５４、およびＩＰ通信プログラム１５５を実行する。

【００５１】

認証プログラム１５１は、パーソナルコンピュータ１などを認証するプログラムである。鍵配信プログラム１５２は、認証されたパーソナルコンピュータ１に、鍵保存プログラム１５３が保存しているコンテンツ鍵を配信するプログラムである。鍵保存プログラム１５３は、鍵生成プログラム１５４により生成されたコンテンツ鍵を保存するプログラムである。鍵生成プログラム１５４は、コンテンツに対応させてコンテンツ鍵を生成するプログラムである。

【００５２】

ＩＰ通信プログラム１５５は、ＨＴＴＰ１７１およびＷａｐ１７２などの手続を包含し、通信ネットワーク４を介して、パーソナルコンピュータ１などと通信するためのプログラムである。

【００５３】

コンテンツサーバ２２－１は、コンテンツ保存プログラム１９１、コンテンツ配信プログラム１９２、およびＩＰ通信プログラム１９３を実行する。

【００５４】

コンテンツ保存プログラム１９１は、暗号化されているコンテンツをコンテンツＩＤと対応させて保存する。コンテンツ配信プログラム１９２は、パーソナルコンピュータ１から要求があったとき、コンテンツ保存プログラム１９１が保存している、コンテンツＩＤに対応するコンテンツをパーソナルコンピュータ１に配信する。

【００５５】

ＩＰ通信プログラム１９３は、ＨＴＴＰ２０１およびＷａｐ２０２などの手続

を包含し、通信ネットワーク４を介して、パーソナルコンピュータ１と通信するためのプログラムである。

【００５６】

ショップサーバ２３－２は、ショップサーバ２３－１と同様の構成を有するので、その説明は省略する。鍵サーバ２１－２は、鍵サーバ２１－１と同様の構成を有するので、その説明は省略する。コンテンツサーバ２２－２は、コンテンツサーバ２２－１と同様の構成を有するのでその説明は省略する。

【００５７】

次に、パーソナルコンピュータ１がサーバ５－１からコンテンツをダウンロードして、ポータブルデバイス２にチェックアウトする従来の処理を図３および図４のフローチャートを参照して説明する。ステップＳ１０１において、パーソナルコンピュータ１のＰＨＳ／ＩＭＴ通信プログラム１５は、公衆回線網３１と接続を確立する。ステップＳ２０１において、公衆回線網３１の図示せぬ地上局などは、パーソナルコンピュータ１と接続を確立する。

【００５８】

ステップＳ１０２において、パーソナルコンピュータ１のＩＳＰ接続プログラム１４は、ＩＳＰ３２と接続を確立する。ステップＳ３０１において、ＩＳＰ３２は、パーソナルコンピュータ１と接続を確立する。

【００５９】

ステップＳ１０３において、パーソナルコンピュータ１のＩＰ通信プログラム１３は、ショップサーバ２３とＩＰ通信を確立する。ステップＳ４０１において、ショップサーバ２３－１のＩＰ通信プログラム１２４は、パーソナルコンピュータ１とＩＰ通信を確立する。

【００６０】

ステップＳ４０２において、ショップサーバ２３－１の閲覧プログラム１２３は、通信ネットワーク４を介して、パーソナルコンピュータ１に閲覧用（コンテンツの選択用）のデジタルデータを送信する。ステップＳ１０４において、パーソナルコンピュータ１の図示せぬブラウザプログラムは、デジタルデータに対応する画像またはテキストなどを表示し、使用者に閲覧させる。また、パーソナル

コンピュータ１のブラウザプログラムは、コンテンツのストリーミング再生によりコンテンツを使用者に試聴させたり、または、キーワードによりコンテンツをショップサーバ２３－１の閲覧プログラム１２３に検索させ、その結果を表示する。ステップＳ４０２およびステップＳ１０４の処理は、パーソナルコンピュータ１の使用者の要求に対応して、繰り返される。

【００６１】

ステップＳ１０５において、パーソナルコンピュータ１のブラウザプログラムは、購入依頼をショップサーバ２３－１に送信する。ステップＳ４０３において、ショップサーバ２３－１の閲覧プログラム１２３は、パーソナルコンピュータ１から送信された購入依頼を受信する。

【００６２】

ステップＳ４０４において、ショップサーバ２３－１のコンテンツ情報送信プログラム１２２は、ステップＳ４０３の処理で受信した購入依頼に対応するコンテンツを配信するコンテンツサーバ２２－１のＵＲＬおよびコンテンツを特定するためのコンテンツＩＤなどを含む、コンテンツ情報を通信ネットワーク４を介してパーソナルコンピュータ１に送信する。ステップＳ１０６において、パーソナルコンピュータ１のコンテンツ情報受信プログラム６７は、ショップサーバ２３－１が送信した、コンテンツ情報を受信する。

【００６３】

ステップＳ４０５において、ショップサーバ２３－１の鍵情報送信プログラム１２１は、ステップＳ４０３の処理で受信した購入依頼に対応するコンテンツのコンテンツ鍵を配信する鍵サーバ２１－１のＵＲＬなどの、鍵情報を通信ネットワーク４を介してパーソナルコンピュータ１に送信する。ステップＳ１０７において、パーソナルコンピュータ１の鍵情報受信プログラム６６は、ショップサーバ２３－１が送信した鍵情報を受信する。

【００６４】

ステップＳ１０８において、パーソナルコンピュータ１のＩＰ通信プログラム１３は、ステップＳ１０６の処理で取得したコンテンツ情報に含まれるコンテンツサーバ２２－１のＵＲＬを基に、コンテンツサーバ２２－１とＩＰ通信を確立

する。ステップＳ５０１において、コンテンツサーバ２２－１のＩＰ通信プログラム１９３は、パーソナルコンピュータ１とＩＰ通信を確立する。

【００６５】

ステップＳ１０９において、パーソナルコンピュータ１のコンテンツ管理プログラム６５は、ステップＳ１０６の処理で取得したコンテンツＩＤを、通信ネットワーク４を介して、コンテンツサーバ２２－１に送信する。ステップＳ５０２において、コンテンツサーバ２２－１は、パーソナルコンピュータ１が送信したコンテンツＩＤを受信する。ステップＳ５０３において、コンテンツサーバ２２－１のコンテンツ配信プログラム１９２は、ステップＳ５０２で受信したコンテンツＩＤに対応するコンテンツ（暗号化されている）をコンテンツ保存プログラム１９１から読み出して、通信ネットワーク４を介して、パーソナルコンピュータ１に配信する。ステップＳ１１０において、パーソナルコンピュータ１のコンテンツ管理プログラム６５の受信プログラム７３は、コンテンツサーバ２２－１が送信したコンテンツを受信する。

【００６６】

ステップＳ１１１において、パーソナルコンピュータ１のＩＰ通信プログラム１３は、ステップＳ１０７の処理で取得した鍵情報に含まれる鍵サーバ２１－１のＵＲＬを基に、鍵サーバ２１－１とＩＰ通信を確立する。ステップＳ６０１において、鍵サーバ２１－１のＩＰ通信プログラム１５５は、パーソナルコンピュータ１とＩＰ通信を確立する。

【００６７】

ステップＳ１１２において、パーソナルコンピュータ１の鍵管理プログラム６４のサーバ認証プログラム７１は、鍵サーバ２１－１を認証する。ステップＳ６０２において、鍵サーバ２１－１の認証プログラム１５１は、パーソナルコンピュータ１を認証する。

【００６８】

鍵サーバ２１－１には、マスター鍵ＫMSが予め記憶されており、パーソナルコンピュータ１には、個別鍵ＫPPとパーソナルコンピュータ１のIDが予め記憶されている。パーソナルコンピュータ１には、更に、マスター鍵ＫMPが予め記憶され

ており、鍵サーバ２１－１にも鍵サーバ２１－１のIDと個別鍵KPSが記憶されている。

【００６９】

鍵サーバ２１－１は、パーソナルコンピュータ１から、パーソナルコンピュータ１のIDの供給を受け、そのIDと自分自身が有するマスター鍵KMSにハッシュ関数を適用して、パーソナルコンピュータ１の個別鍵KPPと同一の鍵を生成する。

【００７０】

パーソナルコンピュータ１は、鍵サーバ２１－１から、鍵サーバ２１－１のIDの供給を受け、そのIDと自分自身が有するマスター鍵KMPにハッシュ関数を適用して、鍵サーバ２１－１の個別鍵KPSと同一の鍵を生成する。このようにすることで、パーソナルコンピュータ１と鍵サーバ２１－１の両方に、共通の個別鍵が共有されることになる。これらの個別鍵を用いてさらに、一時鍵を生成する。

【００７１】

ステップＳ１１３において、パーソナルコンピュータ１の鍵管理プログラム６４は、コンテンツＩＤを鍵サーバ２１－１に送信する。ステップＳ６０３において、鍵サーバ２１－１は、パーソナルコンピュータ１が送信した、コンテンツＩＤを受信する。ステップＳ６０４において、鍵サーバ２１－１の鍵配信プログラム１５２は、鍵保存プログラム１５３がコンテンツＩＤと対応づけて保存しているコンテンツ鍵を読み出し、通信ネットワーク４を介して、そのコンテンツ鍵（一時鍵により暗号化されている）をパーソナルコンピュータ１に送信する。ステップＳ１１４において、パーソナルコンピュータ１の鍵管理プログラム６４の受信プログラム７２は、鍵サーバ２１－１が送信したコンテンツ鍵を受信する。鍵管理プログラム６４は、受信したコンテンツ鍵を一時鍵で復号する。

【００７２】

ステップＳ１１５において、パーソナルコンピュータ１のＰＨＳ／ＩＭＴ通信プログラム１５は、公衆回線網３１との接続を切断する。ステップＳ２０２において、公衆回線網３１の図示せぬ地上局などは、パーソナルコンピュータ１との接続を切断する。

【００７３】

ステップＳ１１６において、フォーマット管理プログラム５３は、ステップＳ１１０の処理で受信したコンテンツの符号化方式および暗号化方式を、それぞれ所定の方式に変換する。

【００７４】

パーソナルコンピュータ１の使用者が、表示操作指示プログラム１１に対し、受信したコンテンツのチェックアウトを指示したとき、ステップＳ１１７以降の処理が実行される。

【００７５】

ステップＳ１１７において、パーソナルコンピュータ１のライセンス管理プログラム５１のPD認証プログラム６３は、ポータブルデバイス２を認証する。ステップＳ７０１において、ポータブルデバイス２のライセンス管理プログラム８１のPC認証プログラム９２は、パーソナルコンピュータ１を認証する。

【００７６】

ステップＳ１１７およびステップＳ７０１におけるパーソナルコンピュータ１とポータブルデバイス２との相互認証の処理は、チャレンジレスポンス方式の認証の処理であり、ステップＳ１１２およびステップＳ６０２における鍵サーバ２１－１とパーソナルコンピュータ１との相互認証の処理に比較して、演算量が少ない。パーソナルコンピュータ１およびポータブルデバイス２は、それぞれ、同一の演算で、レスポンスから一時鍵を生成して、共有する。

【００７７】

ステップＳ１１８において、パーソナルコンピュータ１のコンテンツ管理プログラム６５は、暗号化されているコンテンツをポータブルデバイス２に配信する。ステップＳ７０２において、ポータブルデバイス２のコンテンツ管理プログラム８３は、パーソナルコンピュータ１が配信したコンテンツを受信して、ポータブルメディア３のコンテンツ管理プログラム１０３に供給する。ポータブルメディア３のコンテンツ管理プログラム１０３は、コンテンツを記憶する。

【００７８】

なお、ポータブルデバイス２とポータブルメディア３は、ポータブルデバイス２にポータブルメディア３が装着されたとき、相互認証する。

【００７９】

ステップＳ１１９において、パーソナルコンピュータ１の鍵管理プログラム６４は、ポータブルデバイス２に、ステップＳ１１８で配信したコンテンツに対応するコンテンツ鍵（ポータブルデバイス２とポータブルメディア３とで共有する一時鍵で暗号化されている）を配信する。ステップＳ７０３において、ポータブルデバイス２の鍵管理プログラム８２は、パーソナルコンピュータ１が配信したコンテンツ鍵を受信して、ポータブルメディア３の鍵管理プログラム１０２に供給する。ポータブルメディア３の鍵管理プログラム１０２は、コンテンツ鍵を一時鍵で復号して、コンテンツ鍵を記憶する。

【００８０】

次に、パーソナルコンピュータ１がサーバ５－２からコンテンツをダウンロードして、ポータブルデバイス２にチェックアウトする処理を図５および図６のフローチャートを参照して説明する。ステップＳ１１０１乃至ステップＳ１１０７の処理は、サーバ５－２、並びにＩＰ通信プログラム１３、ＩＳＰ接続プログラム１４、ＰＨＳ／ＩＭＴ通信プログラム１５、およびダウンロードプログラム５２－２により実行され、それぞれ、ステップＳ１０１乃至ステップＳ１０７の処理と同様なので、その説明は省略する。

【００８１】

ステップＳ１１０８において、パーソナルコンピュータ１のＩＰ通信プログラム１３は、ステップＳ１１０７の処理で取得した鍵情報に含まれる鍵サーバ２１－２のＵＲＬを基に、鍵サーバ２１－２とＩＰ通信を確立する。ステップＳ１６０１において、鍵サーバ２１－２は、パーソナルコンピュータ１とＩＰ通信を確立する。

【００８２】

ステップＳ１１０９において、パーソナルコンピュータ１のダウンロードプログラム５２－２は、鍵サーバ２１－２を認証する。ステップＳ１６０２において、鍵サーバ２１－２は、パーソナルコンピュータ１を認証する。ステップＳ１１０９およびステップＳ１６０２の処理は、ステップＳ１１２およびステップＳ６０２の処理と同様の処理である。

【００８３】

ステップＳ１１１０において、パーソナルコンピュータ１のダウンロードプログラム５２－２は、コンテンツＩＤを鍵サーバ２１－２に送信する。ステップＳ１６０３において、鍵サーバ２１－２は、パーソナルコンピュータ１が送信した、コンテンツＩＤを受信する。ステップＳ１６０４において、鍵サーバ２１－２は、コンテンツＩＤと対応づけて保存しているコンテンツ鍵を読み出し、通信ネットワーク４を介して、そのコンテンツ鍵（一時鍵により暗号化されている）をパーソナルコンピュータ１に送信する。ステップＳ１１１１において、パーソナルコンピュータ１のダウンロードプログラム５２－２は、鍵サーバ２１－２が送信したコンテンツ鍵を受信する。ダウンロードプログラム５２－２は、受信したコンテンツ鍵を一時鍵で復号する。

【００８４】

ステップＳ１１１２おいて、パーソナルコンピュータ１のＩＰ通信プログラム１３は、ステップＳ１１０６の処理で取得したコンテンツ情報に含まれるコンテンツサーバ２２－２のＵＲＬを基に、コンテンツサーバ２２－２とＩＰ通信を確立する。ステップＳ１５０１において、コンテンツサーバ２２－２は、パーソナルコンピュータ１とＩＰ通信を確立する。

【００８５】

ステップＳ１１１３において、パーソナルコンピュータ１のダウンロードプログラム５２－２は、ステップＳ１１０６の処理で取得したコンテンツＩＤを、通信ネットワーク４を介して、コンテンツサーバ２２－２に送信する。ステップＳ１５０２において、コンテンツサーバ２２－２は、パーソナルコンピュータ１が送信したコンテンツＩＤを受信する。ステップＳ１５０３において、コンテンツサーバ２２－２は、ステップＳ１５０２で受信したコンテンツＩＤに対応するコンテンツ（暗号化されている）を読み出して、通信ネットワーク４を介して、パーソナルコンピュータ１に配信する。ステップＳ１１１４において、パーソナルコンピュータ１のダウンロードプログラム５２－２は、コンテンツサーバ２２－２が送信したコンテンツを受信する。

【００８６】

ステップＳ１１１５乃至ステップＳ１７０３の処理は、ステップＳ１１５乃至ステップＳ７０３の処理と同様なので、その説明は省略する。

【００８７】

【発明が解決しようとする課題】

以上のように、コンテンツおよびコンテンツ鍵を供給するサーバ５－１または５－２は、それぞれ、コンテンツおよびコンテンツ鍵を供給する手順が異なるので、サーバ５－１および５－２からのコンテンツの受信を所望する場合、サーバ５－１に対応するダウンロードプログラム５２－１とサーバ５－２に対応するダウンロードプログラム５２－２とが必要となる。

【００８８】

しかしながら、コンテンツを受信する装置の、演算能力が小さい、記憶容量が少ないなどの処理能力が小さい場合、コンテンツを受信する装置は、複数のダウンロードプログラムを記憶しておくことができず、ダウンロードプログラムを切り換えて実行することができない。

【００８９】

本発明はこのような状況に鑑みてなされたものであり、処理能力が小さい装置でも、異なる手順で供給されるコンテンツおよび鍵を受信することができるようにすることを目的とする。

【００９０】

【課題を解決するための手段】

請求項１に記載の情報提供装置は、第１の情報処理装置を認証する第１の認証手段と、第２の情報処理装置または第３の情報処理装置を認証する第２の認証手段と、第１の情報処理装置からの、コンテンツおよび鍵の送信要求、並びに第２の情報処理装置を特定するデータまたは第３の情報処理装置を特定するデータの受信を制御する受信制御手段と、第２の情報処理装置を特定するデータを受信した場合、第２の情報処理装置に対応した手順で、第２の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第２の情報処理装置からコンテンツおよび鍵を受信し、第３の情報処理装置を特定するデータを受信した場合、第３の情報処理装置に対応した手順で、第３の情報処理装置にコンテンツおよび鍵の

送信要求を送信するとともに、第３の情報処理装置からコンテンツおよび鍵を受信するように通信を制御する通信制御手段と、第１の情報処理装置へのコンテンツおよび鍵の送信を制御する送信制御手段とを含むことを特徴とする。

【００９１】

情報提供装置は、コンテンツの符号化方式および暗号化方式のうちの少なくとも一方を、所定の符号化方式または暗号化方式に変換する変換手段を更に設けことかできる。

【００９２】

請求項３に記載の情報提供方法は、第１の情報処理装置を認証する第１の認証ステップと、第２の情報処理装置または第３の情報処理装置を認証する第２の認証ステップと、第１の情報処理装置からの、コンテンツおよび鍵の送信要求、並びに第２の情報処理装置を特定するデータまたは第３の情報処理装置を特定するデータの受信を制御する受信制御ステップと、第２の情報処理装置を特定するデータを受信した場合、第２の情報処理装置に対応した手順で、第２の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第２の情報処理装置からコンテンツおよび鍵を受信し、第３の情報処理装置を特定するデータを受信した場合、第３の情報処理装置に対応した手順で、第３の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第３の情報処理装置からコンテンツおよび鍵を受信するように通信を制御する通信制御ステップと、第１の情報処理装置へのコンテンツおよび鍵の送信を制御する送信制御ステップとを含むことを特徴とする。

【００９３】

請求項４に記載のプログラム格納媒体のプログラムは、第１の情報処理装置を認証する第１の認証ステップと、第２の情報処理装置または第３の情報処理装置を認証する第２の認証ステップと、第１の情報処理装置からの、コンテンツおよび鍵の送信要求、並びに第２の情報処理装置を特定するデータまたは第３の情報処理装置を特定するデータの受信を制御する受信制御ステップと、第２の情報処理装置を特定するデータを受信した場合、第２の情報処理装置に対応した手順で、第２の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第

２の情報処理装置からコンテンツおよび鍵を受信し、第３の情報処理装置を特定するデータを受信した場合、第３の情報処理装置に対応した手順で、第３の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第３の情報処理装置からコンテンツおよび鍵を受信するように通信を制御する通信制御ステップと、第１の情報処理装置へのコンテンツおよび鍵の送信を制御する送信制御ステップとを含むことを特徴とする。

【００９４】

請求項５に記載の情報処理装置は、第１の情報提供装置を認証する認証手段と、第１の情報提供装置への、コンテンツおよび鍵の送信要求、並びにコンテンツおよび鍵を提供する第２の情報提供装置を特定するデータ、およびコンテンツおよび鍵を提供する第３の情報提供装置を特定するデータのいずれかの送信を制御する送信制御手段と、第２の情報提供装置または第３の情報提供装置から第１の情報提供装置が提供を受け、送信したコンテンツおよび鍵の受信を制御する受信制御手段とを含むことを特徴とする。

【００９５】

請求項６に記載の情報処理方法は、第１の情報提供装置を認証する認証ステップと、第１の情報提供装置への、コンテンツおよび鍵の送信要求、並びにコンテンツおよび鍵を提供する第２の情報提供装置を特定するデータ、およびコンテンツおよび鍵を提供する第３の情報提供装置を特定するデータのいずれかの送信を制御する送信制御ステップと、第２の情報提供装置または第３の情報提供装置から第１の情報提供装置が提供を受け、送信したコンテンツおよび鍵の受信を制御する受信制御ステップとを含むことを特徴とする。

【００９６】

請求項７に記載のプログラム格納媒体のプログラムは、第１の情報提供装置を認証する認証ステップと、第１の情報提供装置への、コンテンツおよび鍵の送信要求、並びにコンテンツおよび鍵を提供する第２の情報提供装置を特定するデータ、およびコンテンツおよび鍵を提供する第３の情報提供装置を特定するデータのいずれかの送信を制御する送信制御ステップと、第２の情報提供装置または第３の情報提供装置から第１の情報提供装置が提供を受け、送信したコンテンツお

よび鍵の受信を制御する受信制御ステップとを含むことを特徴とする。

【００９７】

請求項１に記載の情報提供装置、請求項３に記載の情報提供方法、および請求項４に記載のプログラム格納媒体においては、第１の情報処理装置が認証され、第２の情報処理装置または第３の情報処理装置が認証され、第１の情報処理装置からの、コンテンツおよび鍵の送信要求、並びに第２の情報処理装置を特定するデータまたは第３の情報処理装置を特定するデータの受信が制御され、第２の情報処理装置を特定するデータを受信した場合、第２の情報処理装置に対応した手順で、第２の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第２の情報処理装置からコンテンツおよび鍵を受信し、第３の情報処理装置を特定するデータを受信した場合、第３の情報処理装置に対応した手順で、第３の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第３の情報処理装置からコンテンツおよび鍵を受信するように通信が制御され、第１の情報処理装置へのコンテンツおよび鍵の送信が制御される。

【００９８】

請求項５に記載の情報処理装置、請求項６に記載の情報処理方法、および請求項７に記載のプログラム格納媒体においては、第１の情報提供装置が認証され、第１の情報提供装置への、コンテンツおよび鍵の送信要求、並びにコンテンツおよび鍵を提供する第２の情報提供装置を特定するデータ、およびコンテンツおよび鍵を提供する第３の情報提供装置を特定するデータのいずれかの送信が制御され、第２の情報提供装置または第３の情報提供装置から第１の情報提供装置が提供を受け、送信したコンテンツおよび鍵の受信が制御される。

【００９９】

【発明の実施の形態】

図７は、本発明に係るデジタルデータ伝送システムの一実施の形態を示す図である。図１で説明した構成の場合と同一の部分には、図１の場合と同一の番号を付してあり、その説明は省略する。

【０１００】

電話機一体型端末機５０１は、ポータブルメディア３－１が装着可能に構成さ

れ、無線により、通信ネットワーク４に接続される。電話機一体型端末機５０１は、通信ネットワーク４を介して、コンテンツサーバ２２－１または２２－２から受信したコンテンツ（所定の方式で圧縮され、暗号化されている）を、利用条件のデータ等と共にダウンロードして、コンテンツおよびその利用条件データを装着されているポータブルメディア３－１に記憶させる。

【０１０１】

電話機一体型端末機５０１は、コンテンツに関連する利用条件のデータに基づいて、装着されているポータブルメディア３－１に記憶されているコンテンツを再生し、図示せぬヘッドフォンまたはスピーカなどに出力する。使用者は、電話機一体型端末機５０１を持ち歩きながら、所望の場所で所望のコンテンツをダウンロードして、そのコンテンツをポータブルメディア３－１に記憶させることができる。使用者は、電話機一体型端末機５０１に、ポータブルメディア３－１に記憶されているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

【０１０２】

電話機一体型端末機５０１の表示操作指示プログラム５１１は、コンテンツに関連するデータ（例えば、曲名、または利用条件など）を表示させるとともに、ダウンロードの指示などを入力して、クライアント用ＬＣＭ５１２にその指示に対応した処理を実行させる。電話機一体型端末機５０１のクライアント用ＬＣＭ５１２は、代理サーバ５０３のサーバ用ＬＣＭ５１４と協同して、利用条件データおよびコンテンツ等をダウンロードする一連の処理（後述する）を実行する。

【０１０３】

電話機一体型端末機５０１のクライアント用ＬＣＭ５１２は、コンテンツの不正な２次利用による著作権の侵害の防止を目的として、個々のコンテンツに対して著作権者が指定する利用条件でのみコンテンツを利用できるように制御を行うモジュール群から構成される。利用条件には、コンテンツの再生条件、コピー条件、移動条件、または蓄積条件などが含まれる。

【０１０４】

クライアント用ＬＣＭ５１２は、電話機一体型端末機５０１に装着されている

ポータブルメディア３－１が正当であるかの認証を行い、安全な方法でサーバ５が指定した利用条件のデータをコンテンツ（暗号化されている）に付加して、ポータブルメディア３－１にコンテンツを記録させる。コンテンツの移動の処理などに伴い、クライアント用ＬＣＭ５１２は、必要な鍵を生成して、鍵を管理し、または接続されているポータブルメディア３－１との通信を制御する。

【０１０５】

パーソナルコンピュータ５０２は、通信ネットワーク４に接続されている。パーソナルコンピュータ５０２は、コンテンツサーバ２２－１若しくは２２－２から受信した、またはCDから読み取ったコンテンツを、所定の圧縮の方式に変換するとともにDESなどの暗号化方式で暗号化して記録する。パーソナルコンピュータ５０２は、暗号化して記録しているコンテンツに対応して、コンテンツの利用条件を示す利用条件のデータを記録する。

【０１０６】

パーソナルコンピュータ５０２の表示操作指示プログラム１１は、コンテンツに関連するデータ（例えば、曲名、または利用条件など）を表示させるとともに、ダウンロード、またはチェックアウトの指示などを入力して、ＬＣＭ５１３にその指示に対応したダウンロード、またはチェックアウトなどの処理を実行させる。

【０１０７】

パーソナルコンピュータ５０２のＬＣＭ５１３は、コンテンツの不正な２次利用による著作権の侵害の防止を目的として、個々のコンテンツに対して著作権者が指定する利用条件でのみコンテンツを利用できるように制御を行うモジュール群から構成される。利用条件には、コンテンツの再生条件、コピー条件、移動条件、または蓄積条件などが含まれる。

【０１０８】

ＬＣＭ５１３は、パーソナルコンピュータ５０２に接続されたポータブルデバイス２が正当であるかの認証を行い、安全な方法でコンテンツの移動の処理などを実行する。コンテンツの移動の処理などに伴い、ＬＣＭ５１３は、必要な鍵を生成して、鍵を管理し、コンテンツを暗号化し、または接続されている機器との

通信を制御する。

【０１０９】

また、ＬＣＭ５１３は、ポータブルデバイス２の正当性をチェックする。ポータブルデバイス２は、ポータブルメディア３－２が装着されたとき、ポータブルメディア３－２の正当性をチェックする。ポータブルデバイス２およびポータブルメディア３－２が正当である場合、ＬＣＭ５１３は、サーバ５が指定した利用条件のデータをコンテンツ（暗号化されている）に付加して、ポータブルメディア３－２にコンテンツをチェックアウトする。ポータブルデバイス２は、パーソナルコンピュータ５０２からチェックアウトされたコンテンツを、コンテンツに関連するデータと共に、装着されているポータブルメディア３－２に記憶させる。

【０１１０】

パーソナルコンピュータ５０２のＬＣＭ５１３は、暗号化して記録しているコンテンツを、接続されているポータブルデバイス２にチェックアウトする。ポータブルデバイス２は、パーソナルコンピュータ５０２からチェックアウトされたコンテンツを、コンテンツに関連するデータと共に、装着されているポータブルメディア３－２に記憶させる。

【０１１１】

代理サーバ５０３を利用できるとき、パーソナルコンピュータ５０２のＰＣ用ＬＣＭ５２１（ＬＣＭ５１３の一部または全部の機能から構成される）は、代理サーバ５０３のサーバ用ＬＣＭ５１４と協同して、利用条件データおよびコンテンツ等をダウンロードする一連の処理を実行する。

【０１１２】

代理サーバ５０３を利用できないとき、パーソナルコンピュータ５０２のＬＣＭ５１３は、ＬＣＭ１２と同様の鍵サーバ２１－１または２１－２との認証の処理等を実行して、利用条件データおよびコンテンツ等をダウンロードする。

【０１１３】

代理サーバ５０３は、サーバ用ＬＣＭ５１４を実行して、相互認証した電話機一体型端末機５０１または相互認証したパーソナルコンピュータ５０２の要求に

対応して、鍵サーバ２１－１または２１－２との認証の処理を実行する。代理サーバ５０３は、鍵サーバ２１－１または２１－２との相互認証の処理の後、鍵サーバ２１－１または２１－２からコンテンツ鍵を受信して、受信したコンテンツ鍵を電話機一体型端末機５０１またはパーソナルコンピュータ５０２に供給する。代理サーバ５０３は、コンテンツサーバ２２－１または２２－２からコンテンツを受信して、受信したコンテンツを電話機一体型端末機５０１またはパーソナルコンピュータ５０２に供給する。

【０１１４】

代理サーバ５０３は、サーバ５－１からコンテンツおよびコンテンツ鍵をダウンロードするとき、サーバ５－１からコンテンツを受信した後、コンテンツ鍵を受信する。代理サーバ５０３は、サーバ５－２からコンテンツおよびコンテンツ鍵をダウンロードするとき、コンテンツ鍵を受信した後、コンテンツを受信する。

【０１１５】

代理サーバ５０３は、サーバ５－１からコンテンツおよびコンテンツ鍵をダウンロードしたときも、サーバ５－２からコンテンツおよびコンテンツ鍵をダウンロードしたときも、いずれの場合も、同一の手順（例えば、コンテンツ鍵を送信してから、コンテンツを送信する）で、電話機一体型端末機５０１またはパーソナルコンピュータ５０２にコンテンツおよびコンテンツ鍵を供給する。

【０１１６】

電話機一体型端末機５０１またはパーソナルコンピュータ５０２は、代理サーバ５０３を介して、サーバ５－１または５－２からコンテンツおよびコンテンツ鍵をダウンロードすることにより、同一の手順でコンテンツおよびコンテンツ鍵を受信することができる。

【０１１７】

図８は、電話機一体型端末機５０１の構成を説明する図である。CPU（Central Processing Unit）６０１は、ROM（Read-only Memory）６０２またはRAM（Random-Access Memory）６０３に格納されている各種プログラムを実際に実行する。ROM６０２は、EEPROM（Electrically Erasable Programmable Read-Only Memory

）またはフラッシュメモリなどで構成され、一般的には、CPU６０１が使用するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。RAM６０３は、SRAM（Static RAM）などで構成され、CPU６０１の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。

【０１１８】

入力部６０５は、入力キーまたはマイクロフォンなどで構成され、CPU６０１に各種の指令を入力するとき、または音声などを入力するとき、使用者により操作される。表示部６０６は、液晶表示装置などから成り、各種情報をテキストやイメージで表示する。

【０１１９】

音声再生部６０７は、通信部６０８から供給された通話相手の音声のデータ、またはインターフェース６０９から供給されたポータブルメディア３－１に記憶されているコンテンツを再生して、音声を出力する。

【０１２０】

通信部６０８は、公衆回線網３１と接続し、CPU６０１から供給されたデータ（例えば、コンテンツの送信要求など）または入力部６０５から供給された使用者の音声のデータを、所定の方式のパケットに格納して、公衆回線網３１を介して、送信する。また、通信部６０８は、公衆回線網３１を介して、受信したパケットに格納されているデータ（例えば、コンテンツなど）または通話相手の音声のデータをCPU６０１、RAM６０３、音声再生部６０７、またはインターフェース６０９に出力する。

【０１２１】

インターフェース６０９は、CPU６０１、RAM６０３、または通信部６０８から供給されたデータを装着されているポータブルメディア３－１に記憶させるとともに、装着されているポータブルメディア３－１からコンテンツなどのデータを読み出して、CPU６０１、RAM６０３、または音声再生部６０７に供給する。

【０１２２】

インターフェース６１０は、外付けのドライブ６３１が接続される。ドライブ６３１は、装着されている磁気ディスク６４１、光ディスク６４２（CD-ROMを含

む）、光磁気ディスク６４３、または半導体メモリ６４４に記録されているデータまたはプログラムを読み出して、そのデータまたはプログラムを、インターフェース６１０、およびバス６０４を介して接続されているROM６０２またはRAM６０３に供給する。

【０１２３】

CPU６０１乃至インターフェース６１０は、バス６０４により相互に接続されている。

【０１２４】

図９は、代理サーバ５０３の構成を説明する図である。CPU６５１は、各種アプリケーションプログラム（詳細については後述する）や、OS（Operating System)を実際に実行する。ROM６５２は、一般的には、CPU６５１が使用するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。RAM６５３は、CPU６５１の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。これらはCPUバスなどから構成されるホストバス６５４により相互に接続されている。

【０１２５】

ホストバス６５４は、ブリッジ６５５を介して、PCI(Peripheral Component Interconnect/Interface)バスなどの外部バス６５６に接続されている。

【０１２６】

キーボード６５８は、CPU６５１に各種の指令を入力するとき、使用者により操作される。ポインティングデバイス６５９は、ディスプレイ６６０の画面上のポイントの指示や選択を行うとき、使用者により操作される。ディスプレイ６６０は、液晶表示装置またはCRT（Cathode Ray Tube）などから成り、各種情報をテキストやイメージで表示する。HDD（Hard Disk Drive）６６１は、ハードディスクを駆動し、それらにCPU６５１によって実行するプログラムや情報を記録または再生させる。

【０１２７】

ドライブ６６２は、装着されている磁気ディスク６８１、光ディスク６８２、光磁気ディスク６８３、または半導体メモリ６８４に記録されているデータまた

はプログラムを読み出して、そのデータまたはプログラムを、インターフェース６５７、外部バス６５６、ブリッジ６５５、およびホストバス６５４を介して接続されているRAM６５３に供給する。

【０１２８】

これらのキーボード６５８乃至ドライブ６６２は、インターフェース６５７に接続されており、インターフェース６５７は、外部バス６５６、ブリッジ６５５、およびホストバス６５４を介してCPU６５１に接続されている。

【０１２９】

通信部６６３は、通信ネットワーク４が接続され、CPU６５１、またはHDD６６１から供給されたデータ（例えば、コンテンツ鍵など）を、所定の方式のパケットに格納して、通信ネットワーク４を介して、送信するとともに、通信ネットワーク４を介して、受信したパケットに格納されているデータ（例えば、コンテンツＩＤなど）をCPU６５１、RAM６５３、またはHDD６６１に出力する。

【０１３０】

通信部６６３は、外部バス６５６、ブリッジ６５５、およびホストバス６５４を介してCPU６５１に接続されている。

【０１３１】

次に、図１０を参照して、本願のデジタルデータ伝送システムの機能の構成について説明する。図２で説明した構成の場合と同一の部分には、図２の場合と同一の番号を付してあり、その説明は省略する。

【０１３２】

電話機一体型端末機５０１は、表示操作指示プログラム５１１、クライアント用ＬＣＭ５１２、ＩＰ通信プログラム７０１、ＩＳＰ接続プログラム７０２、およびＰＨＳ／ＩＭＴ通信プログラム７０３を実行する。

【０１３３】

ＰＨＳ／ＩＭＴ通信プログラム７０３は、公衆回線網３１を介して通信を行うためのプログラムである。ＩＳＰ接続プログラム７０２は、ＩＳＰ３２と接続するためのプログラムである。ＩＰ通信プログラム７０１は、ＨＴＴＰ７４１およびＷａｐ７４２などの手続を包含し、通信ネットワーク４を介して、鍵サーバ２

１－１、コンテンツサーバ２２－１、ショップサーバ２３－１、鍵サーバ２１－２、コンテンツサーバ２２－２、ショップサーバ２３－２、または代理サーバ５０３などと通信するためのプログラムである。

【０１３４】

クライアント用ＬＣＭ５１２は、ライセンス管理プログラム７１１、ダウンロードプログラム７１２、およびフォーマット管理プログラム７１３などから構成されている。

【０１３５】

ライセンス管理プログラム７１１は、コンテンツの利用条件に基づいたコンテンツの利用を管理するためのプログラムであり、利用条件管理プログラム７２１、サーバ認証プログラム７２２、およびPM認証プログラム７２３などから構成されている。

【０１３６】

利用条件管理プログラム７２１は、コンテンツの利用条件に基づいて、ポータブルメディア３－１が記憶しているコンテンツの再生などを許可するか、または禁止するかなどの管理を実行するとともに、ポータブルメディア３－１が記憶しているコンテンツの再生などに対応して、ポータブルメディア３－１に、ポータブルメディア３－１が記憶している利用条件のデータを更新させる。サーバ認証プログラム７２２は、通信ネットワーク４を介して、代理サーバ５０３を認証する。PM認証プログラム７２３は、ポータブルメディア３－１が電話機一体型端末機５０１に装着されたとき、ポータブルメディア３－１を認証する。

【０１３７】

ダウンロードプログラム７１２は、鍵管理プログラム７２４、コンテンツ管理プログラム７２５、鍵情報受信プログラム７２６、およびコンテンツ情報受信プログラム７２７などから構成されている。

【０１３８】

鍵管理プログラム７２４は、代理サーバ５０３からコンテンツ鍵を受信して、コンテンツに対応させて、コンテンツ鍵をポータブルメディア３－１に記憶させて、管理する。鍵管理プログラム７２４は、代理サーバ５０３からコンテンツ鍵

を受信する受信プログラム７３１などを含む。

【０１３９】

コンテンツ管理プログラム７２５は、代理サーバ５０３からコンテンツの利用条件とともにコンテンツ（暗号化されている）を受信して、コンテンツの利用条件とともにコンテンツをポータブルメディア３－１に記憶させる。コンテンツ管理プログラム７２５の受信プログラム７３２は、代理サーバ５０３からコンテンツの利用条件およびコンテンツを受信する。

【０１４０】

鍵情報受信プログラム７２６は、ショップサーバ２３－１または２３－２から、コンテンツに対応するコンテンツ鍵を供給する鍵サーバ２１－１または２１－２を特定するＵＲＬを受信する。コンテンツ情報受信プログラム７２７は、ショップサーバ２３－１または２３－２から、所望のコンテンツを特定するコンテンツＩＤ、および所望のコンテンツを供給するコンテンツサーバ２２－１または２２－２を特定するＵＲＬを受信する。

【０１４１】

フォーマット管理プログラム７１３は、代理サーバ５０３を介して、コンテンツサーバ２２－１または２２－２からダウンロードしたコンテンツの符号化方式および暗号化方式をそれぞれ所定の方式に変換する。フォーマット管理プログラム７１３は、システム識別プログラム７２８およびフォーマット変換プログラム７２９などから構成されている。

【０１４２】

システム識別プログラム７２８は、コンテンツのダウンロード先が、サーバ５－１であるか、サーバ５－２であるかのいずれかを識別するためのプログラムである。フォーマット変換プログラム７２９は、コンテンツの符号化方式および暗号化方式を変換する。

【０１４３】

次に、代理サーバ５０３の構成について説明する。代理サーバ５０３は、サーバ用ＬＣＭ５１４、およびＩＰ通信プログラム７５１を実行する。

【０１４４】

サーバ用ＬＣＭ５１４は、ライセンス管理プログラム７６１、およびシーケンス管理プログラム７６２などを含む。

【０１４５】

ライセンス管理プログラム７６１は、更に、鍵サーバ２１－１または２１－２を認証するサーバ認証プログラム７８１、および電話機一体型端末機５０１を認証するＰＤ認証プログラム７８２などを含む。

【０１４６】

シーケンス管理プログラム７６２は、鍵管理プログラム７７１、コンテンツ管理プログラム７７２、およびシステム識別プログラム７７３などを含む。

【０１４７】

鍵管理プログラム７７１は、更に、通信ネットワーク４を介して、鍵サーバ２１－１または２１－２からコンテンツ鍵を受信する鍵受信プログラム７８３、および通信ネットワーク４を介して、受信したコンテンツ鍵を電話機一体型端末機５０１に配信する鍵配信プログラム７８４などを含む。

【０１４８】

コンテンツ管理プログラム７７２は、更に、通信ネットワーク４を介して、コンテンツサーバ２２－１または２２－２からコンテンツを受信するコンテンツ受信プログラム７８５、および通信ネットワーク４を介して、受信したコンテンツを電話機一体型端末機５０１に配信するコンテンツ配信プログラム７８６などを含む。

【０１４９】

システム識別プログラム７７３は、電話機一体型端末機５０１から供給されたコンテンツＩＤを基に、コンテンツのダウンロード先が、サーバ５－１であるか、サーバ５－２であるかのいずれかを識別するためのプログラムである。

【０１５０】

ＩＰ通信プログラム７５１は、ＨＴＴＰ７８７およびＷａｐ７８８などの手続を包含し、通信ネットワーク４を介して、サーバ５－１若しくは５－２、または電話機一体型端末機５０１と通信するためのプログラムである。

【０１５１】

次に、電話機一体型端末機５０１がサーバ５－１からコンテンツをダウンロードする処理を図１１および図１２のフローチャートを参照して説明する。ステップＳ２１０１において、電話機一体型端末機５０１のＰＨＳ／ＩＭＴ通信プログラム７０３は、公衆回線網３１と接続を確立する。ステップＳ２２０１において、公衆回線網３１の図示せぬ地上局などは、電話機一体型端末機５０１と接続を確立する。

【０１５２】

ステップＳ２１０２において、電話機一体型端末機５０１のＩＳＰ接続プログラム７０２は、電話機一体型端末機５０１と公衆回線網３１との接続を介して、ＩＳＰ３２と接続を確立する。ステップＳ２３０１において、ＩＳＰ３２は、電話機一体型端末機５０１と公衆回線網３１との接続を介して、電話機一体型端末機５０１と接続を確立する。

【０１５３】

以降の電話機一体型端末機５０１と、鍵サーバ２１－１、コンテンツサーバ２２－１、ショップサーバ２３－１、または代理サーバ５０３との処理は、電話機一体型端末機５０１とＩＳＰ３２との接続を介して実行される。

【０１５４】

ステップＳ２１０３において、電話機一体型端末機５０１のＩＰ通信プログラム７０１は、ショップサーバ２３－１とＩＰ通信を確立する。ステップＳ２４０１において、ショップサーバ２３－１のＩＰ通信プログラム１２４は、電話機一体型端末機５０１とＩＰ通信を確立する。

【０１５５】

ステップＳ２４０２において、ショップサーバ２３－１の閲覧プログラム１２３は、通信ネットワーク４を介して、電話機一体型端末機５０１に閲覧用（コンテンツの選択用）のデジタルデータを送信する。ステップＳ２１０４において、電話機一体型端末機５０１の図示せぬブラウザプログラムは、受信したデジタルデータに対応するテキストまたは画像を表示部６０６に表示させ、使用者に閲覧させる。また、電話機一体型端末機５０１のブラウザプログラムは、コンテンツのストリーミング再生により、コンテンツを音声再生部６０７に再生させて、使

用者に試聴させたり、または、キーワードにより所望のコンテンツをショップサーバ２３－１の閲覧プログラム１２３に検索させ、その結果を表示部６０６に表示させる。

【０１５６】

ステップＳ２４０２およびステップＳ２１０４の処理は、電話機一体型端末機５０１の使用者の要求に対応して、例えば、使用者が購入するコンテンツを決定するまで繰り返される。

【０１５７】

ステップＳ２１０５において、電話機一体型端末機５０１のブラウザプログラムは、通信ネットワーク４を介して、購入依頼をショップサーバ２３－１に送信する。ステップＳ２４０３において、ショップサーバ２３－１の閲覧プログラム１２３は、電話機一体型端末機５０１から送信された購入依頼を受信する。

【０１５８】

ステップＳ２４０４において、ショップサーバ２３－１のコンテンツ情報送信プログラム１２２は、ステップＳ２４０３の処理で受信した購入依頼に対応して、コンテンツを配信するコンテンツサーバ２２－１のＵＲＬ、およびコンテンツを特定するためのコンテンツＩＤなどを含む、コンテンツ情報を、通信ネットワーク４を介して、電話機一体型端末機５０１に送信する。ステップＳ２１０６において、電話機一体型端末機５０１のコンテンツ情報受信プログラム７２７は、ショップサーバ２３－１が送信した、コンテンツ情報を受信する。

【０１５９】

ステップＳ２４０５において、ショップサーバ２３－１の鍵情報送信プログラム１２１は、ステップＳ２４０３の処理で受信した購入依頼に対応するコンテンツのコンテンツ鍵を配信する鍵サーバ２１－１のＵＲＬなどの、鍵情報を通信ネットワーク４を介して、電話機一体型端末機５０１に送信する。ステップＳ２１０７において、電話機一体型端末機５０１の鍵情報受信プログラム７２６は、ショップサーバ２３－１が送信した、鍵情報を受信する。

【０１６０】

ステップＳ２１０８において、電話機一体型端末機５０１のＩＰ通信プログラ

ム７０１は、予め記録している代理サーバ５０３のＵＲＬを基に、代理サーバ５０３とＩＰ通信を確立する。ステップＳ２５０１において、代理サーバ５０３のＩＰ通信プログラム７５１は、電話機一体型端末機５０１とＩＰ通信を確立する。

【０１６１】

ステップＳ２１０９において、電話機一体型端末機５０１のライセンス管理プログラム７１１のサーバ認証プログラム７２２は、代理サーバ５０３を認証する。ステップＳ２５０２において、代理サーバ５０３のライセンス管理プログラム７６１のPD認証プログラム７８２は、電話機一体型端末機５０１を認証する。

【０１６２】

ステップＳ２１０９およびステップＳ２５０２における電話機一体型端末機５０１と代理サーバ５０３との相互認証の処理は、チャレンジレスポンス方式の認証の処理であり、ステップＳ１１２およびステップＳ６０２における鍵サーバ２１－１とパーソナルコンピュータ１との相互認証の処理に比較して、演算量が少なく、少ない演算能力、または記憶容量でも、迅速に実行することができる。電話機一体型端末機５０１および代理サーバ５０３は、それぞれ、同一の演算で、レスポンスから一時鍵を生成して、共有する。

【０１６３】

ステップＳ２１０９およびステップＳ２５０２における認証の処理に失敗したとき（認証の相手が正当でないと判定されたとき）、電話機一体型端末機５０１がコンテンツをダウンロードする処理は、コンテンツをダウンロードしないで、終了する。

【０１６４】

ステップＳ２１１０において、電話機一体型端末機５０１のコンテンツ管理プログラム７２５は、コンテンツＩＤを代理サーバ５０３に送信する。ステップＳ２５０３において、代理サーバ５０３は、電話機一体型端末機５０１が送信したコンテンツＩＤを受信する。ステップＳ２１１１において、電話機一体型端末機５０１の鍵管理プログラム７２４は、ステップＳ２１０７の処理で受信した鍵情報を代理サーバ５０３に送信する。ステップＳ２５０４において、代理サーバ５

０３は、電話機一体型端末機５０１が送信した、鍵情報を受信する。

【０１６５】

ステップＳ２５０５において、代理サーバ５０３のシステム識別プログラム７７３は、ステップＳ２５０３の処理で受信したコンテンツＩＤを基に、コンテンツおよびコンテンツ鍵のダウンロード先が、サーバ５－１であることを識別する。

【０１６６】

なお、ステップＳ２１１０において、電話機一体型端末機５０１は、コンテンツＩＤと共にコンテンツサーバ２２－１のＵＲＬを送信して、ステップＳ２５０３において、代理サーバ５０３は、コンテンツＩＤと共にコンテンツサーバ２２－１のＵＲＬを受信するようにしてもよい。

【０１６７】

ステップＳ２５０６において、代理サーバ５０３のＩＰ通信プログラム７５１は、ステップＳ２５０５の処理の識別の結果を基に、コンテンツサーバ２２－１とＩＰ通信を確立する。ステップＳ２６０１において、コンテンツサーバ２２－１のＩＰ通信プログラム１９３は、代理サーバ５０３とＩＰ通信を確立する。

【０１６８】

ステップＳ２５０７において、代理サーバ５０３のコンテンツ管理プログラム７７２は、ステップＳ２５０３の処理で取得したコンテンツＩＤを、通信ネットワーク４を介して、コンテンツサーバ２２－１に送信する。ステップＳ２６０２において、コンテンツサーバ２２－１は、代理サーバ５０３が送信したコンテンツＩＤを受信する。ステップＳ２６０３において、コンテンツサーバ２２－１のコンテンツ配信プログラム１９２は、ステップＳ２６０２で受信したコンテンツＩＤに対応するコンテンツ（暗号化されている）を、コンテンツ保存プログラム１９１から読み出して、通信ネットワーク４を介して、代理サーバ５０３に配信する。

【０１６９】

ステップＳ２５０８において、代理サーバ５０３のコンテンツ管理プログラム７７２の受信プログラム７８５は、コンテンツサーバ２２－１が送信したコンテ

ンツを受信する。

【０１７０】

ステップＳ２５０９において、代理サーバ５０３のＩＰ通信プログラム７５１は、ステップＳ２５０５の処理の識別の結果を基に、鍵サーバ２１－１とＩＰ通信を確立する。ステップＳ２７０１において、鍵サーバ２１－１のＩＰ通信プログラム１５５は、代理サーバ５０３とＩＰ通信を確立する。

【０１７１】

ステップＳ２５１０において、代理サーバ５０３のライセンス管理プログラム７６１のサーバ認証プログラム７８１は、鍵サーバ２１－１を認証する。ステップＳ２７０２において、鍵サーバ２１－１の認証プログラム１５１は、代理サーバ５０３を認証する。

【０１７２】

例えば、鍵サーバ２１－１には、マスター鍵ＫMSSが予め記憶されており、代理サーバ５０３には、個別鍵ＫPCCと代理サーバ５０３のIDが予め記憶されている。代理サーバ５０３には、更に、マスター鍵ＫMCCが予め記憶されており、鍵サーバ２１－１にも鍵サーバ２１－１のIDと個別鍵ＫPSSが記憶されている。

【０１７３】

鍵サーバ２１－１は、代理サーバ５０３から、代理サーバ５０３のIDの供給を受け、そのIDと自分自身が有するマスター鍵ＫMSSにハッシュ関数を適用して、代理サーバ５０３の個別鍵ＫPCCと同一の鍵を生成する。

【０１７４】

代理サーバ５０３は、鍵サーバ２１－１から、鍵サーバ２１－１のIDの供給を受け、そのIDと自分自身が有するマスター鍵ＫMCCにハッシュ関数を適用して、鍵サーバ２１－１の個別鍵ＫPSSと同一の鍵を生成する。このようにすることで、代理サーバ５０３と鍵サーバ２１－１の両方に、共通の個別鍵が共有されることになる。これらの個別鍵を用いてさらに、一時的な一時鍵を生成する。

【０１７５】

ステップＳ２５１０またはステップＳ２７０２における認証の処理に失敗したとき（認証の相手が正当でないと判定されたとき）、処理は終了する。

【０１７６】

ステップＳ２５１１において、代理サーバ５０３の鍵管理プログラム７７１は、ステップＳ２５０３の処理で取得したコンテンツＩＤを鍵サーバ２１－１に送信する。ステップＳ２７０３において、鍵サーバ２１－１は、代理サーバ５０３が送信したコンテンツＩＤを受信する。ステップＳ２７０４において、鍵サーバ２１－１の鍵配信プログラム１５２は、鍵保存プログラム１５３がコンテンツＩＤと対応づけて保存しているコンテンツ鍵を読み出し、通信ネットワーク４を介して、そのコンテンツ鍵（鍵サーバ２１－１と代理サーバ５０３とで共有する一時鍵で暗号化されている）を代理サーバ５０３に送信する。ステップＳ２５１２において、代理サーバ５０３の鍵管理プログラム７７１の鍵受信プログラム７８３は、鍵サーバ２１－１が送信したコンテンツ鍵を受信する。

【０１７７】

ステップＳ２５１３において、代理サーバ５０３の鍵管理プログラム７７１の鍵配信プログラム７８４は、ステップＳ２５１２の処理で受信したコンテンツ鍵を、鍵サーバ２１－１と代理サーバ５０３とで共有する一時鍵で復号し、電話機一体型端末機５０１と代理サーバ５０３で共有する一時鍵で暗号化して、通信ネットワーク４を介して、暗号化されているコンテンツ鍵を電話機一体型端末機５０１に送信する。ステップＳ２１１２において、電話機一体型端末機５０１の鍵管理プログラム７２４の受信プログラム７３１は、代理サーバ５０３が送信したコンテンツ鍵を受信する。鍵管理プログラム７２４は、コンテンツ鍵を電話機一体型端末機５０１と代理サーバ５０３で共有する一時鍵で復号して、ポータブルメディア３－１の鍵管理プログラム１０２に供給し、鍵管理プログラム１０２に、コンテンツ鍵を記憶させる。

【０１７８】

ステップＳ２５１４において、代理サーバ５０３のコンテンツ管理プログラム７７２のコンテンツ配信プログラム７８６は、通信ネットワーク４を介して、暗号化されているコンテンツを電話機一体型端末機５０１に送信する。ステップＳ２１１３において、電話機一体型端末機５０１のコンテンツ管理プログラム７２５の受信プログラム７３２は、代理サーバ５０３が送信したコンテンツを受信す

る。

【０１７９】

ステップＳ２１１４において、電話機一体型端末機５０１のＰＨＳ／ＩＭＴ通信プログラム７０３は、公衆回線網３１との接続を切断する。ステップＳ２２０２において、公衆回線網３１の図示せぬ地上局などは、電話機一体型端末機５０１と接続を切断する。

【０１８０】

ステップＳ２１１５において、電話機一体型端末機５０１のフォーマット管理プログラム７１３は、ステップＳ２１１３の処理で受信したコンテンツのフォーマットを変換する。コンテンツ管理プログラム７２５は、フォーマットを変換したコンテンツを、インターフェース６０９を介して、ポータブルメディア３－１に供給して、コンテンツ管理プログラム１０３に、コンテンツを記憶させ、処理は終了する。

【０１８１】

次に、電話機一体型端末機５０１がサーバ５－２からコンテンツをダウンロードする処理を図１３および図１４のフローチャートを参照して説明する。ステップＳ３１０１乃至ステップＳ３５０４の処理は、サーバ５－２、並びにＩＰ通信プログラム７０１、ＩＳＰ接続プログラム７０２、ＰＨＳ／ＩＭＴ通信プログラム７０３、およびダウンロードプログラム７１２により実行され、それぞれ、ステップＳ２１０１乃至ステップＳ２５０４の処理と同様なので、その説明は省略する。

【０１８２】

ステップＳ３５０５において、代理サーバ５０３のシステム識別プログラム７７３は、ステップＳ３５０３の処理で受信したコンテンツＩＤを基に、コンテンツおよびコンテンツ鍵のダウンロード先が、サーバ５－２であることを識別する。

【０１８３】

ステップＳ３５０６において、代理サーバ５０３のＩＰ通信プログラム７５１は、ステップＳ３５０５の識別の処理の結果を基に、鍵サーバ２１－２とＩＰ通

信を確立する。ステップＳ３７０１において、鍵サーバ２１－２は、代理サーバ５０３とＩＰ通信を確立する。

【０１８４】

ステップＳ３５０７において、代理サーバ５０３のサーバ認証プログラム７８１は、鍵サーバ２１－２を認証する。ステップＳ３７０２において、鍵サーバ２１－２は、代理サーバ５０３を認証する。

【０１８５】

ステップＳ３５０７およびステップＳ３７０２の処理は、ステップＳ２５１０およびステップＳ２７０２の処理と同様の処理である。

【０１８６】

ステップＳ３５０７またはステップＳ３７０２における認証の処理に失敗したとき（認証の相手が正当でないと判定されたとき）、処理は終了する。

【０１８７】

ステップＳ３５０８において、代理サーバ５０３の鍵管理プログラム７７１は、ステップＳ３５０３の処理で取得したコンテンツＩＤを鍵サーバ２１－２に送信する。ステップＳ３７０３において、鍵サーバ２１－２は、代理サーバ５０３が送信したコンテンツＩＤを受信する。ステップＳ３７０４において、鍵サーバ２１－２は、コンテンツＩＤと対応づけて保存しているコンテンツ鍵を読み出し、通信ネットワーク４を介して、そのコンテンツ鍵（鍵サーバ２１－２と代理サーバ５０３とで共有する一時鍵で暗号化されている）を代理サーバ５０３に送信する。ステップＳ３５０９において、代理サーバ５０３の鍵管理プログラム７７１の鍵受信プログラム７８３は、鍵サーバ２１－２が送信したコンテンツ鍵を受信する。

【０１８８】

ステップＳ３５１０において、代理サーバ５０３のＩＰ通信プログラム７５１は、ステップＳ３５０５の識別の処理の結果を基に、コンテンツサーバ２２－２とＩＰ通信を確立する。ステップＳ３６０１において、コンテンツサーバ２２－２は、代理サーバ５０３とＩＰ通信を確立する。

【０１８９】

ステップＳ３５１１において、代理サーバ５０３のコンテンツ管理プログラム７７２は、ステップＳ３５０３の処理で取得したコンテンツＩＤを、通信ネットワーク４を介して、コンテンツサーバ２２－２に送信する。ステップＳ３６０２において、コンテンツサーバ２２－２は、代理サーバ５０３が送信したコンテンツＩＤを受信する。ステップＳ３６０３において、コンテンツサーバ２２－２は、ステップＳ３６０２で受信したコンテンツＩＤに対応するコンテンツ（暗号化されている）を読み出して、通信ネットワーク４を介して、代理サーバ５０３に配信する。

【０１９０】

ステップＳ３５１２において、代理サーバ５０３のコンテンツ管理プログラム７７２の受信プログラム７８５は、コンテンツサーバ２２－２が送信したコンテンツを受信する。

【０１９１】

ステップＳ３５１２乃至ステップＳ３１１５の処理は、ステップＳ２５１３乃至ステップＳ２１１５の処理と同様なので、その説明は省略する。

【０１９２】

以上のように、電話機一体型端末機５０１は、代理サーバ５０３を介することにより、サーバ５－１からコンテンツおよびコンテンツ鍵をダウンロードするときも、サーバ５－２からコンテンツおよびコンテンツ鍵をダウンロードするときも、いずれの場合も、同一の手順（例えば、コンテンツ鍵を受信してから、コンテンツを受信する）で、コンテンツおよびコンテンツ鍵を受信することができる。

【０１９３】

また、図１１乃至図１４のフローチャートを参照して説明した手順は、後述する代理サーバ５０３がコンテンツの符号化方式および暗号化方式を変換する処理（図１６および図１７のフローチャートを参照して説明する）に比較して、電話機一体型端末機５０１が公衆回線網３１に接続している時間を短くすることができる。

【０１９４】

次に、図１５を参照して、本願のデジタルデータ伝送システムの他の機能の構成について説明する。図１０で説明した構成の場合と同一の部分には、図１０の場合と同一の番号を付してあり、その説明は省略する。

【０１９５】

図１５に示す電話機一体型端末機５０１は、フォーマット管理プログラム７１３を有しない。

【０１９６】

図１５に示す代理サーバ５０３のサーバ用ＬＣＭ５１４は、ライセンス管理プログラム７６１およびシーケンス管理プログラム７６２に加えて、フォーマット管理プログラム８０１を含む。

【０１９７】

フォーマット管理プログラム８０１は、コンテンツサーバ２２－１または２２－２からダウンロードしたコンテンツの符号化方式および暗号化方式をそれぞれ所定の方式に変換する。フォーマット管理プログラム８０１は、システム識別プログラム８１１およびフォーマット変換プログラム８１２から構成されている。

【０１９８】

システム識別プログラム８１１は、コンテンツのダウンロード先が、サーバ５－１であるか、サーバ５－２であるかのいずれかを識別するためのプログラムである。フォーマット変換プログラム８１２は、コンテンツの符号化方式および暗号化方式を変換する。

【０１９９】

次に、図１５にその構成を示す電話機一体型端末機５０１および代理サーバ５０３がサーバ５－２からコンテンツをダウンロードする処理を図１６および図１７のフローチャートを参照して説明する。

【０２００】

ステップＳ４１０１乃至ステップＳ４５１２の処理は、それぞれ、ステップＳ３１０１乃至ステップＳ３５１２の処理と同様なので、その説明は省略する。

【０２０１】

ステップＳ４５１２において、代理サーバ５０３のフォーマット管理プログラ

ム８０１は、ステップＳ４５１２の処理で受信したコンテンツのフォーマットを変換する。

【０２０２】

ステップＳ４５１４において、代理サーバ５０３の鍵管理プログラム７７１の鍵配信プログラム７８４は、ステップＳ４５０９の処理で受信したコンテンツ鍵を、鍵サーバ２１－２と代理サーバ５０３とで共有する一時鍵で復号し、電話機一体型端末機５０１と代理サーバ５０３で共有する一時鍵で暗号化して、通信ネットワーク４を介して、暗号化されているコンテンツ鍵を電話機一体型端末機５０１に送信する。ステップＳ４１１２において、電話機一体型端末機５０１の鍵管理プログラム７２４の受信プログラム７３１は、代理サーバ５０３が送信したコンテンツ鍵を受信する。鍵管理プログラム７２４は、コンテンツ鍵を電話機一体型端末機５０１と代理サーバ５０３で共有する一時鍵で復号して、ポータブルメディア３－１の鍵管理プログラム１０２に供給し、鍵管理プログラム１０２に、コンテンツ鍵を記憶させる。

【０２０３】

ステップＳ４５１５において、代理サーバ５０３のコンテンツ管理プログラム７７２のコンテンツ配信プログラム７８６は、通信ネットワーク４を介して、暗号化されているコンテンツを電話機一体型端末機５０１に送信する。ステップＳ４１１３において、電話機一体型端末機５０１のコンテンツ管理プログラム７２５の受信プログラム７３２は、代理サーバ５０３が送信したコンテンツを受信する。コンテンツ管理プログラム７２５は、受信したコンテンツ（フォーマットが変換されている）を、インターフェース６０９を介して、ポータブルメディア３－１に供給して、コンテンツ管理プログラム１０３に、コンテンツを記憶させる。

【０２０４】

ステップＳ４１１４において、電話機一体型端末機５０１のＰＨＳ／ＩＭＴ通信プログラム７０３は、公衆回線網３１との接続を切断する。ステップＳ４２０２において、公衆回線網３１の図示せぬ地上局などは、電話機一体型端末機５０１と接続を切断して、処理は終了する。

【０２０５】

なお、サーバ５－１からコンテンツおよびコンテンツ鍵を受信する処理は、代理サーバ５０３がサーバ５－１よりコンテンツを受信した後、サーバ５－１よりコンテンツ鍵を受信する手順となり、同様に行われる。

【０２０６】

このように、代理サーバ５０３は、サーバ５－１または５－２から受信したコンテンツの符号化方式および暗号化方式を変換して、電話機一体型端末機５０１に供給することもできる。この場合、電話機一体型端末機５０１は、コンテンツの符号化方式および暗号化方式を変換するプログラムが不要となる。従って、電話機一体型端末機５０１は、図１０に示す場合に比較して、より少ない演算能力または記憶容量でも、迅速にコンテンツを受信する処理を実行することができる。

【０２０７】

また、コンテンツは、楽音のデータであると説明したが、楽音のデータに限らず、静止画像のデータ、動画像のデータ、テキストのデータ、またはプログラムなどでもよい。

【０２０８】

なお、電話機一体型端末機５０１またはパーソナルコンピュータ５０２が、コンテンツをダウンロードすると説明したが、電話機一体型端末機５０１またはパーソナルコンピュータ５０２に限らず、携帯電話機、ＰＤＡ（Personal Digital Assistant）、通信機能付き撮像機能付きデジタルビデオカセットレコーダ、通信機能付き電子手帳装置、または携帯型パーソナルコンピュータなどがコンテンツをダウンロードするようにしてもよい。

【０２０９】

また、電話機一体型端末機５０１は、ＰＨＳまたはＩＭＴにより通信すると説明したが、ＰＨＳまたはＩＭＴに限らず、W-CDMA（Code Division Multiple Access）、衛星通信、衛星放送、PSTN（Public Switched telephone network）、xDSL（x Digital Subscriber Line）、ISDN（Integrated Services Digital Network）、またはプライベートネットワークなどで通信するようにしてもよい。

【０２１０】

上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、プログラム格納媒体からインストールされる。

【０２１１】

コンピュータにインストールされ、コンピュータによって実行可能な状態とされるプログラムを格納するプログラム格納媒体は、図８または図９に示すように、磁気ディスク６４１若しくは磁気ディスク６８１（いずれもフロッピディスクを含む）、光ディスク６４２若しくは光ディスク６８２（いずれも、CD-ROM(Compact Disc-Read Only Memory)、ＤＶＤ(Digital Versatile Disc)を含む）、光磁気ディスク６４３若しくは光磁気ディスク６８３（いずれもＭＤ(Mini-Disc)を含む）、若しくは半導体メモリ６４４若しくは半導体メモリ６８４などよりなるパッケージメディア、または、プログラムが一時的若しくは永続的に格納されるROM６０２若しくはROM６５２や、HDD６６１などにより構成される。プログラム格納媒体へのプログラムの格納は、必要に応じて通信部６０８または通信部６６３を介して、ローカルエリアネットワーク、インターネット、デジタル衛星放送といった、有線または無線の通信媒体を利用して行われる。

【０２１２】

なお、本明細書において、プログラム格納媒体に格納されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【０２１３】

また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【０２１４】

【発明の効果】

請求項１に記載の情報提供装置、請求項３に記載の情報提供方法、および請求項４に記載のプログラム格納媒体によれば、第１の情報処理装置が認証され、第２の情報処理装置または第３の情報処理装置が認証され、第１の情報処理装置からの、コンテンツおよび鍵の送信要求、並びに第２の情報処理装置を特定するデータまたは第３の情報処理装置を特定するデータの受信が制御され、第２の情報処理装置を特定するデータを受信した場合、第２の情報処理装置に対応した手順で、第２の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第２の情報処理装置からコンテンツおよび鍵を受信し、第３の情報処理装置を特定するデータを受信した場合、第３の情報処理装置に対応した手順で、第３の情報処理装置にコンテンツおよび鍵の送信要求を送信するとともに、第３の情報処理装置からコンテンツおよび鍵を受信するように通信が制御され、第１の情報処理装置へのコンテンツおよび鍵の送信が制御されるようにしたので、第１の情報処理装置の処理能力が小さくとも、異なる手順で供給されるコンテンツおよび鍵を受信することができるようになる。

【０２１５】

請求項５に記載の情報処理装置、請求項６に記載の情報処理方法、および請求項７に記載のプログラム格納媒体によれば、第１の情報提供装置が認証され、第１の情報提供装置への、コンテンツおよび鍵の送信要求、並びにコンテンツおよび鍵を提供する第２の情報提供装置を特定するデータ、およびコンテンツおよび鍵を提供する第３の情報提供装置を特定するデータのいずれかの送信が制御され、第２の情報提供装置または第３の情報提供装置から第１の情報提供装置が提供を受け、送信したコンテンツおよび鍵の受信が制御されるようにしたので、処理能力が小さくとも、異なる手順で供給されるコンテンツおよび鍵を受信することができるようになる。

【図面の簡単な説明】

【図１】

従来のデジタルデータ伝送システムの構成を示す図である。

【図２】

従来のデジタルデータ伝送システムの機能の構成を示す図である。

【図３】

パーソナルコンピュータ１がサーバ５－１からコンテンツをダウンロードして、ポータブルデバイス２にチェックアウトする従来の処理を説明するフローチャートである。

【図４】

パーソナルコンピュータ１がサーバ５－１からコンテンツをダウンロードして、ポータブルデバイス２にチェックアウトする従来の処理を説明するフローチャートである。

【図５】

パーソナルコンピュータ１がサーバ５－２からコンテンツをダウンロードして、ポータブルデバイス２にチェックアウトする従来の処理を説明するフローチャートである。

【図６】

パーソナルコンピュータ１がサーバ５－２からコンテンツをダウンロードして、ポータブルデバイス２にチェックアウトする従来の処理を説明するフローチャートである。

【図７】

本発明に係るデジタルデータ伝送システムの一実施の形態を示す図である。

【図８】

電話機一体型端末機５０１の構成を説明する図である。

【図９】

代理サーバ５０３の構成を説明する図である。

【図１０】

本願のデジタルデータ伝送システムの機能の構成を説明する図である。

【図１１】

電話機一体型端末機５０１がサーバ５－１からコンテンツをダウンロードする処理を説明するフローチャートである。

【図１２】

電話機一体型端末機５０１がサーバ５－１からコンテンツをダウンロードする処理を説明するフローチャートである。

【図１３】

電話機一体型端末機５０１がサーバ５－２からコンテンツをダウンロードする処理を説明するフローチャートである。

【図１４】

電話機一体型端末機５０１がサーバ５－２からコンテンツをダウンロードする処理を説明するフローチャートである。

【図１５】

本願のデジタルデータ伝送システムの他の機能の構成を説明する図である。

【図１６】

電話機一体型端末機５０１がサーバ５－２からコンテンツをダウンロードする処理を説明するフローチャートである。

【図１７】

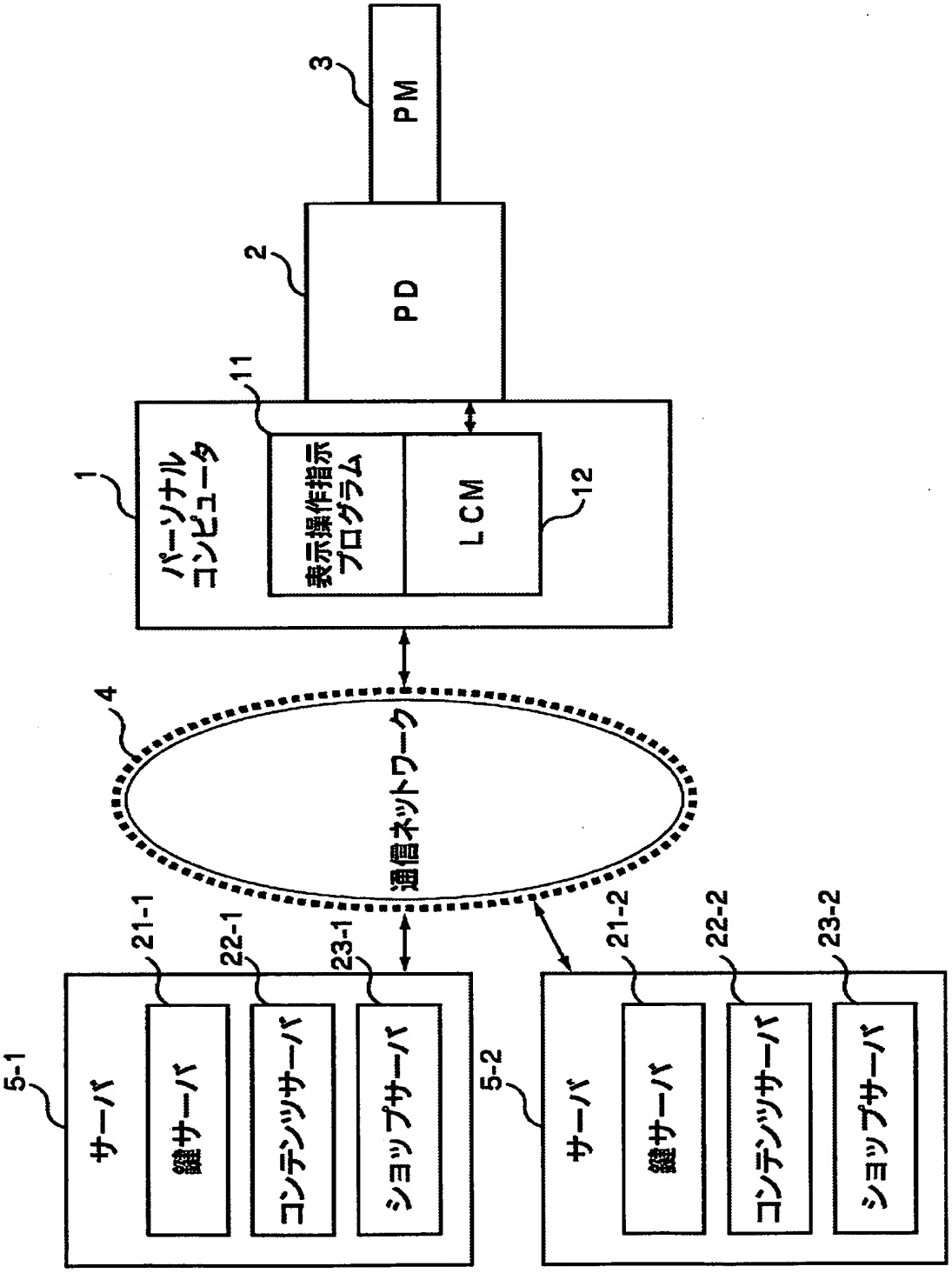
電話機一体型端末機５０１がサーバ５－２からコンテンツをダウンロードする処理を説明するフローチャートである。

【符号の説明】

５０１　電話機一体型端末機，　５０３　代理サーバ，　５１１　表示操作指示プログラム，　５１２　クライアント用ＬＣＭ，　５１４　サーバ用ＬＣＭ，　６０１　ＣＰＵ，　６０２　ＲＯＭ，　６０３　ＲＡＭ，　６０８　通信部，　６４１　磁気ディスク，　６４２　光ディスク，　６４３　光磁気ディスク，　６４４　半導体メモリ，　６５１　ＣＰＵ，　６５２　ＲＯＭ，　６５３　ＲＡＭ，　６６３　通信部，　６８１　磁気ディスク，　６８２　光ディスク，　６８３　光磁気ディスク，　６８４　半導体メモリ

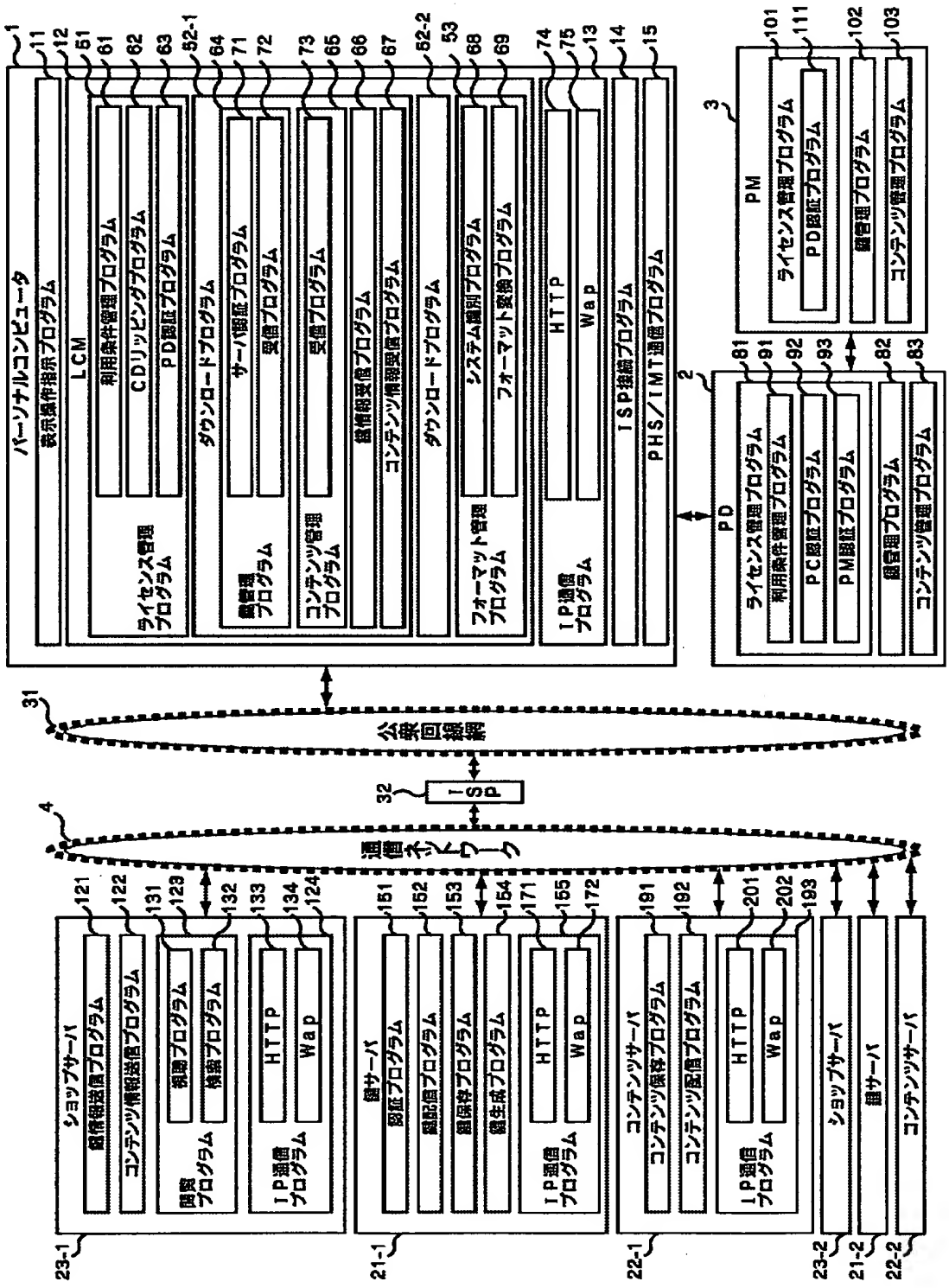
【書類名】図面

【図１】



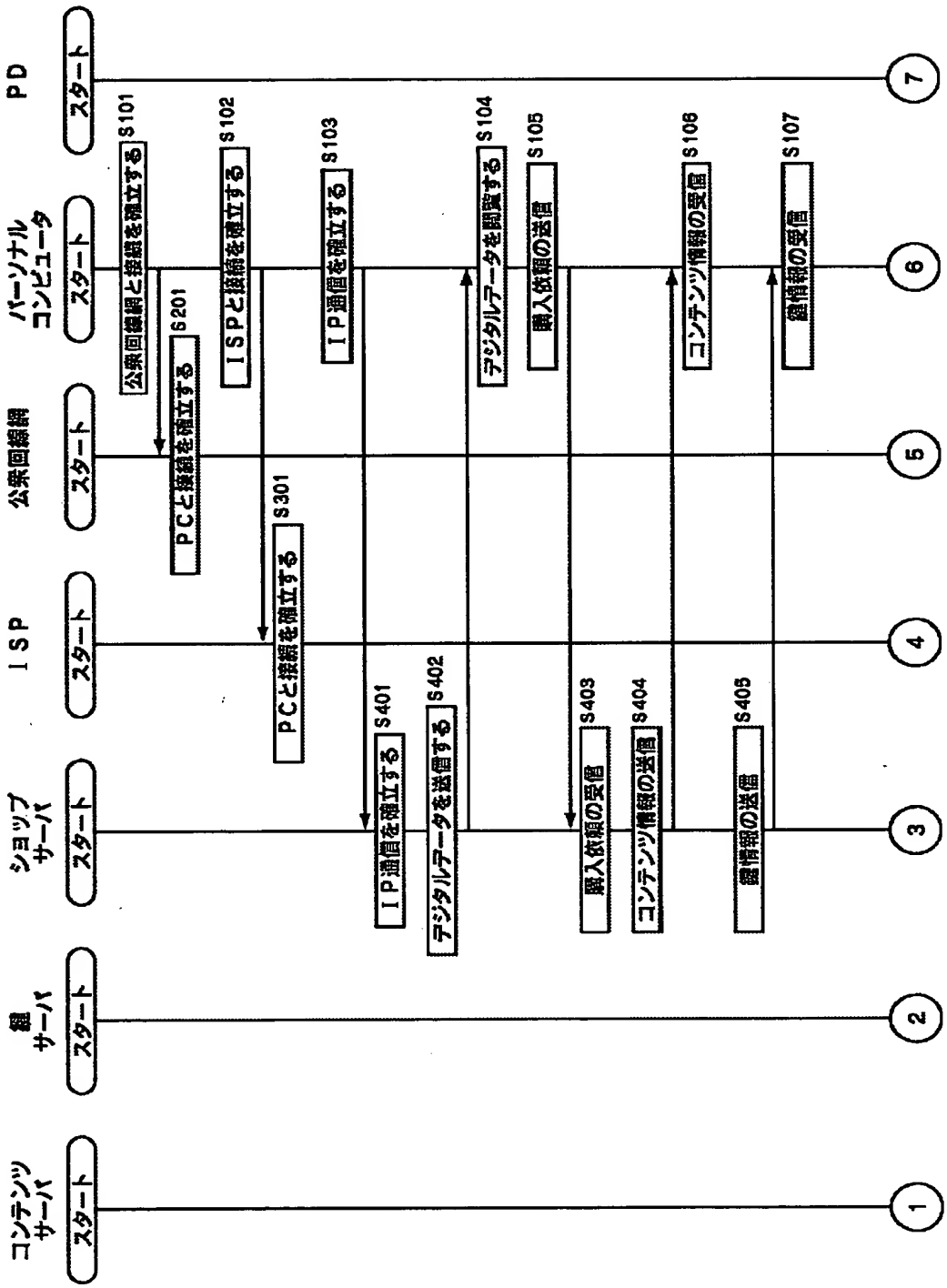
出証特２０００－３１０６１４６

【図２】


パーソナルコンピュータ
表示操作指示プログラム
LCM
ライセンス管理プログラム
利用条件管理プログラム
CDリッピングプログラム
PD固定プログラム
ダウンロードプログラム
課金管理プログラム
サーバ側処プログラム
受信プログラム
コンテンツ管理プログラム
受信プログラム
課情報受信プログラム
コンテンツ情報受信プログラム
ダウンロードプログラム
フォーマット管理プログラム
システム個別プログラム
フォーマット変換プログラム
IP通信プログラム
HTTP
Wap
ISP接続プログラム
PHS／IMT通信プログラム
PD
ライセンス管理プログラム
利用条件管理プログラム
PC固定プログラム
PM固定プログラム
課金管理プログラム
コンテンツ管理プログラム
PM
ライセンス管理プログラム
PD固定プログラム
課金管理プログラム
コンテンツ管理プログラム
公衆回線網
ISP
通信ネットワーク
ショップサーバ
課情報送信プログラム
コンテンツ情報送信プログラム
課題プログラム
情報プログラム
IP通信プログラム
HTTP
Wap
課サーバ
課固定プログラム
課配信プログラム
課保存プログラム
課生成プログラム
IP通信プログラム
HTTP
Wap
コンテンツサーバ
コンテンツ保存プログラム
コンテンツ配信プログラム
IP通信プログラム
HTTP
Wap
ショップサーバ
課サーバ
コンテンツサーバ

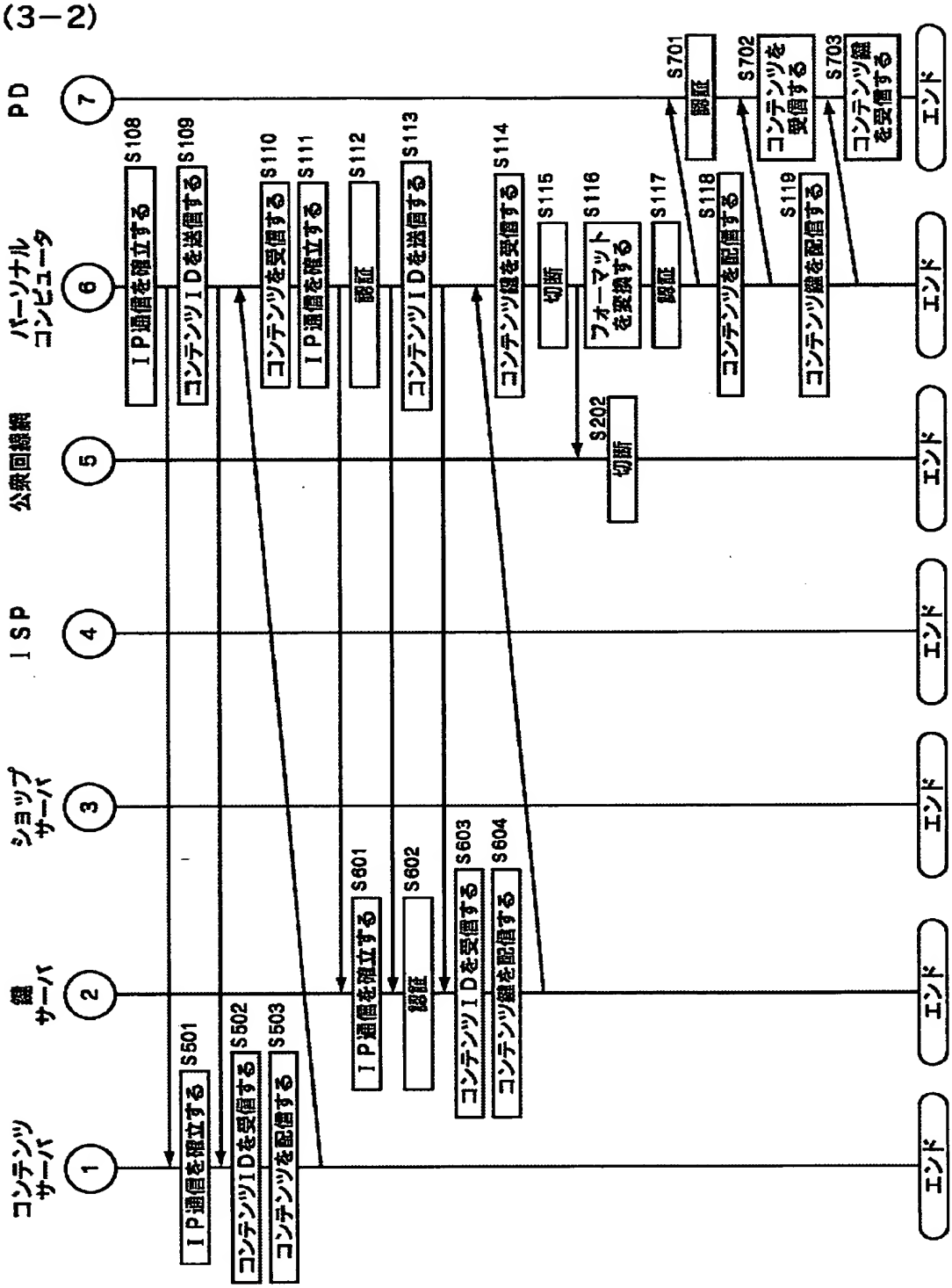
【図３】

(3－1)


PD
パーソナルコンピュータ
公衆回線網
ISP
ショップサーバ
銀サーバ
コンテンツサーバ
スタート
公衆回線と接続を確立する
S101
PCと接続を確立する
S201
ISPと接続を確立する
S102
PCと接続を確立する
S301
IP通信を確立する
S103
IP通信を確立する
S401
デジタルデータを送信する
S402
デジタルデータを閲覧する
S104
購入依頼の送信
S105
購入依頼の受信
S403
コンテンツ情報の送信
S404
コンテンツ情報の受信
S106
課情報の送信
S405
課情報の受信
S107
1
2
3
4
5
6
7

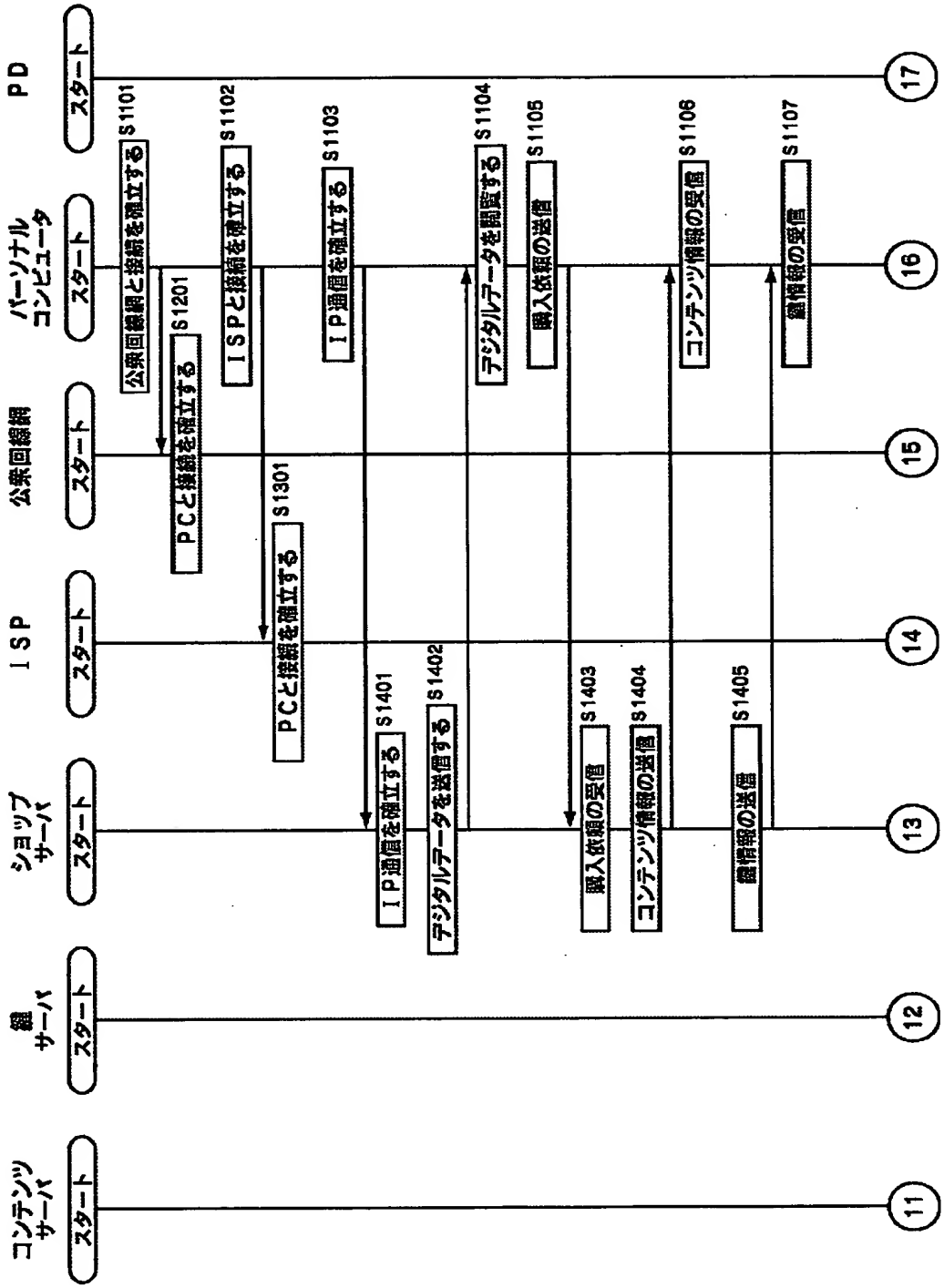
【図４】

(3－2)

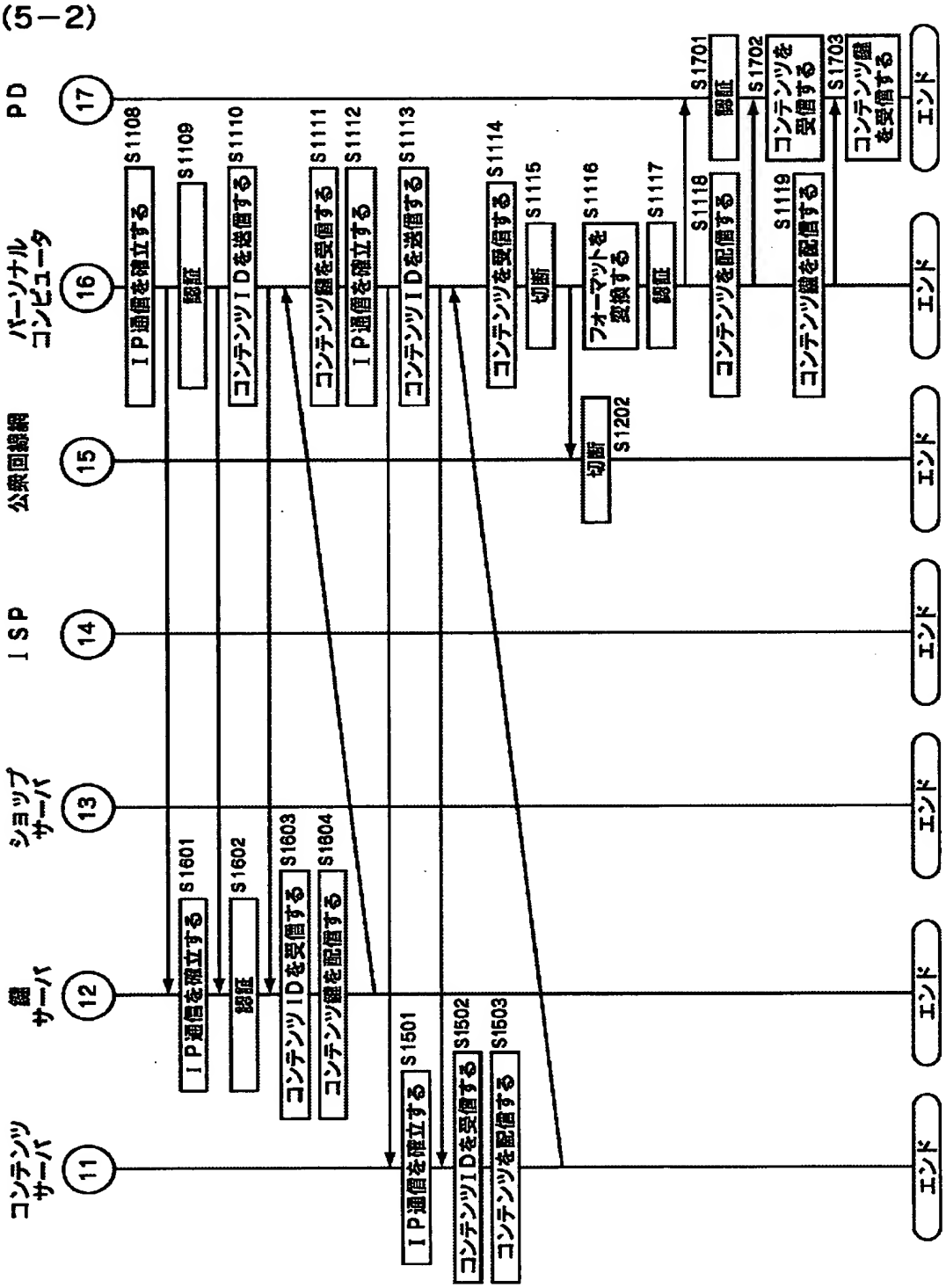

コンテンツサーバ
鍵サーバ
ショップサーバ
ISP
公衆回線網
パーソナルコンピュータ
PD
エンド
IP通信を確立する
コンテンツIDを送信する
コンテンツを受信する
IP通信を確立する
認証
コンテンツIDを送信する
コンテンツ鍵を受信する
切断
フォーマットを変換する
認証
コンテンツを配信する
コンテンツ鍵を配信する
認証
コンテンツを受信する
コンテンツ鍵を受信する
IP通信を確立する
コンテンツIDを受信する
コンテンツを配信する
IP通信を確立する
認証
コンテンツIDを受信する
コンテンツ鍵を配信する
切断
S108
S109
S110
S111
S112
S113
S114
S115
S116
S117
S118
S119
S701
S702
S703
S501
S502
S503
S601
S602
S603
S604
S202

【図５】

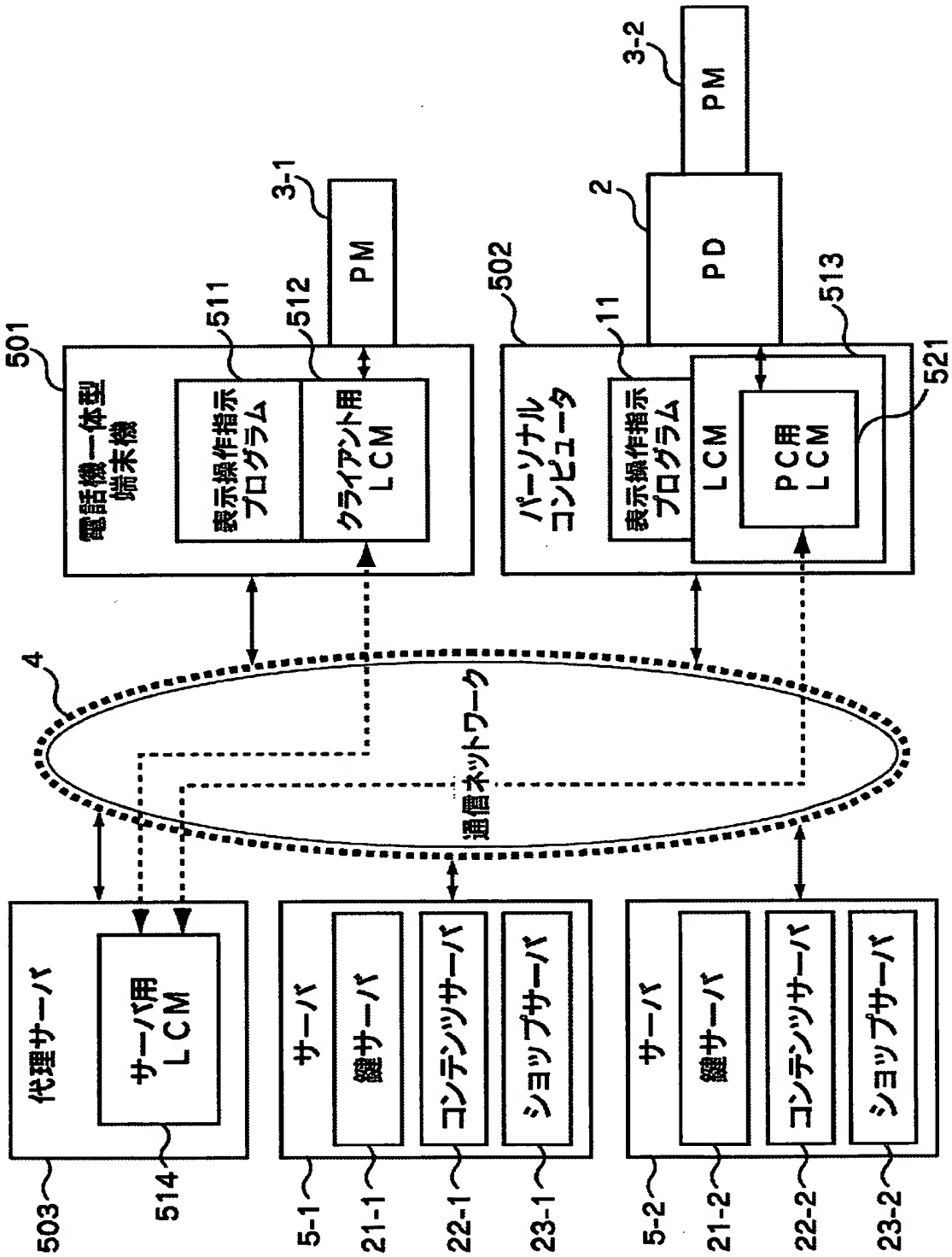
(5－1)


PD
パーソナルコンピュータ
公衆回線網
ISP
ショップサーバ
銀サーバ
コンテンツサーバ
スタート
公衆回線網と接続を確立する
S1101
PCと接続を確立する
S1201
ISPと接続を確立する
S1102
PCと接続を確立する
S1301
IP通信を確立する
S1103
IP通信を確立する
S1401
デジタルデータを送信する
S1402
デジタルデータを開設する
S1104
購入依頼の送信
S1105
購入依頼の受信
S1403
コンテンツ情報の送信
S1404
コンテンツ情報の受信
S1106
書情報の送信
S1405
書情報の受信
S1107
17
16
15
14
13
12
11

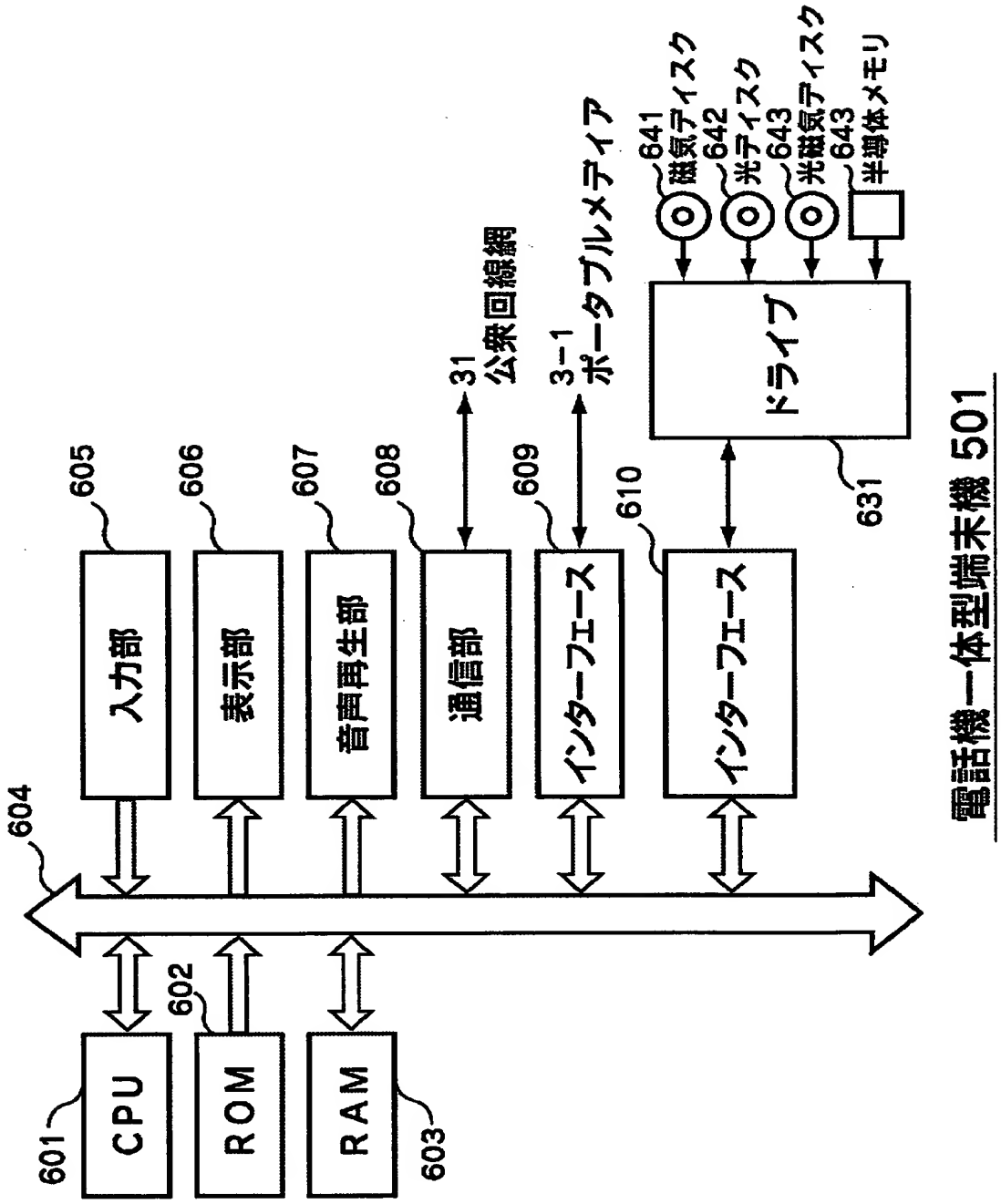
【図６】


(5－2)
PD
パーソナル コンピュータ
公衆回線網
ISP
ショップ サーバ
鍵 サーバ
コンテンツ サーバ
17
16
15
14
13
12
11
S1108
IP通信を確立する
S1109
認証
S1110
コンテンツIDを送信する
S1111
コンテンツ鍵を受信する
S1112
IP通信を確立する
S1113
コンテンツIDを送信する
S1114
コンテンツを受信する
S1115
切断
S1116
フォーマットを変換する
S1117
認証
S1118
コンテンツを配信する
S1119
コンテンツ鍵を配信する
S1701
認証
S1702
コンテンツを受信する
S1703
コンテンツ鍵を受信する
エンド
切断
S1202
S1601
IP通信を確立する
S1602
認証
S1603
コンテンツIDを受信する
S1604
コンテンツ鍵を配信する
S1501
IP通信を確立する
S1502
コンテンツIDを受信する
S1503
コンテンツを配信する

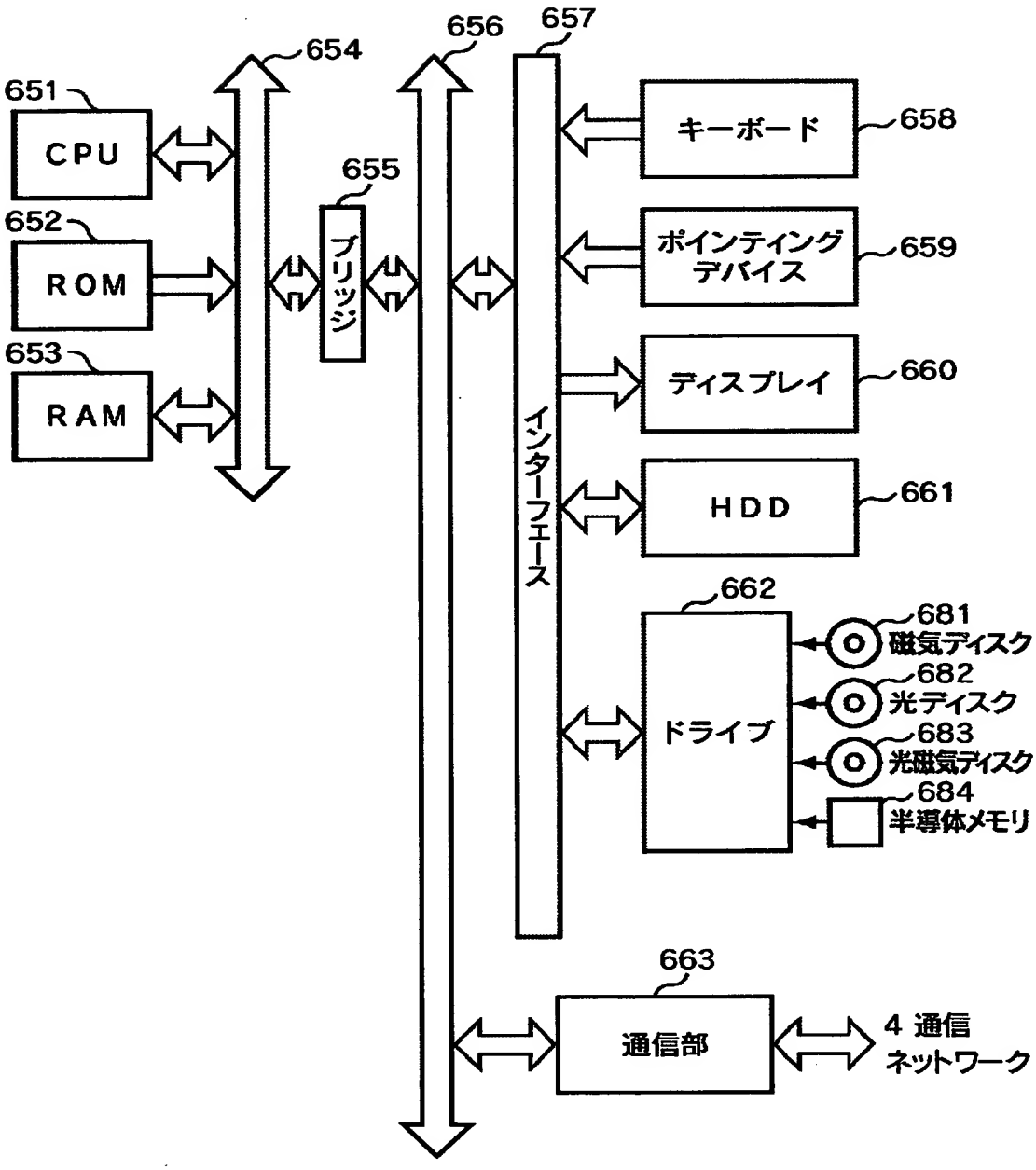
【図７】


501
電話機一体型端末機
511
表示操作指示プログラム
512
クライアント用LCM
3-1
PM
502
パーソナルコンピュータ
11
表示操作指示プログラム
513
LCM
521
PC用LCM
2
PD
3-2
PM
4
通信ネットワーク
代理サーバ
サーバ用LCM
503
514
サーバ
鍵サーバ
コンテンツサーバ
ショップサーバ
5-1
21-1
22-1
23-1
サーバ
鍵サーバ
コンテンツサーバ
ショップサーバ
5-2
21-2
22-2
23-2

【図８】

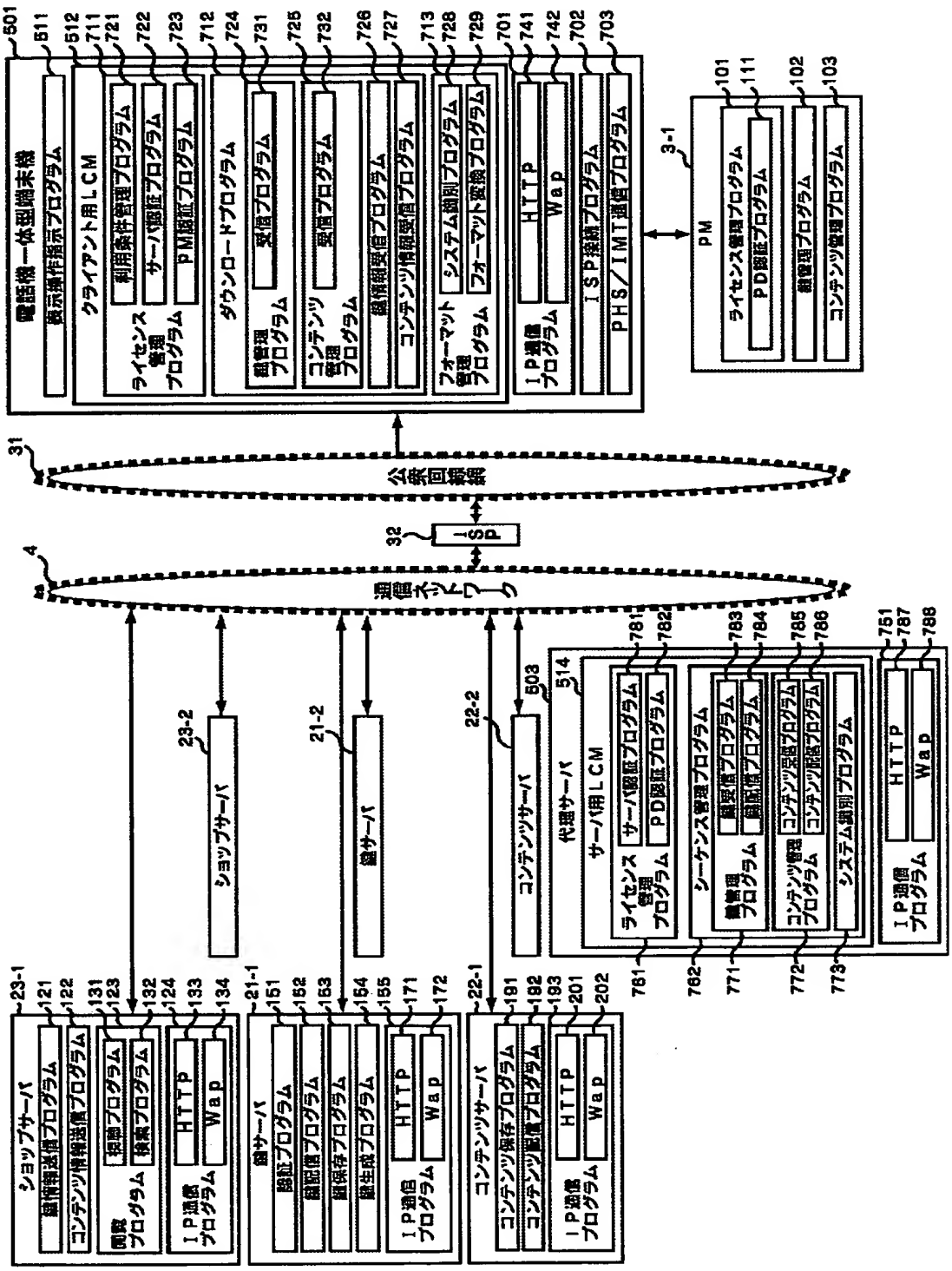

電話機一体型端末機 501
CPU
ROM
RAM
入力部
表示部
音声再生部
通信部
インターフェース
インターフェース
ドライブ
601
602
603
604
605
606
607
608
609
610
631
31
公衆回線網
3-1
ポータブルメディア
641
磁気ディスク
642
光ディスク
643
光磁気ディスク
643
半導体メモリ

【図９】


651
CPU
652
ROM
653
RAM
654
655
ブリッジ
656
657
インターフェース
キーボード
658
ポインティングデバイス
659
ディスプレイ
660
HDD
661
662
ドライブ
681
磁気ディスク
682
光ディスク
683
光磁気ディスク
684
半導体メモリ
663
通信部
4 通信ネットワーク

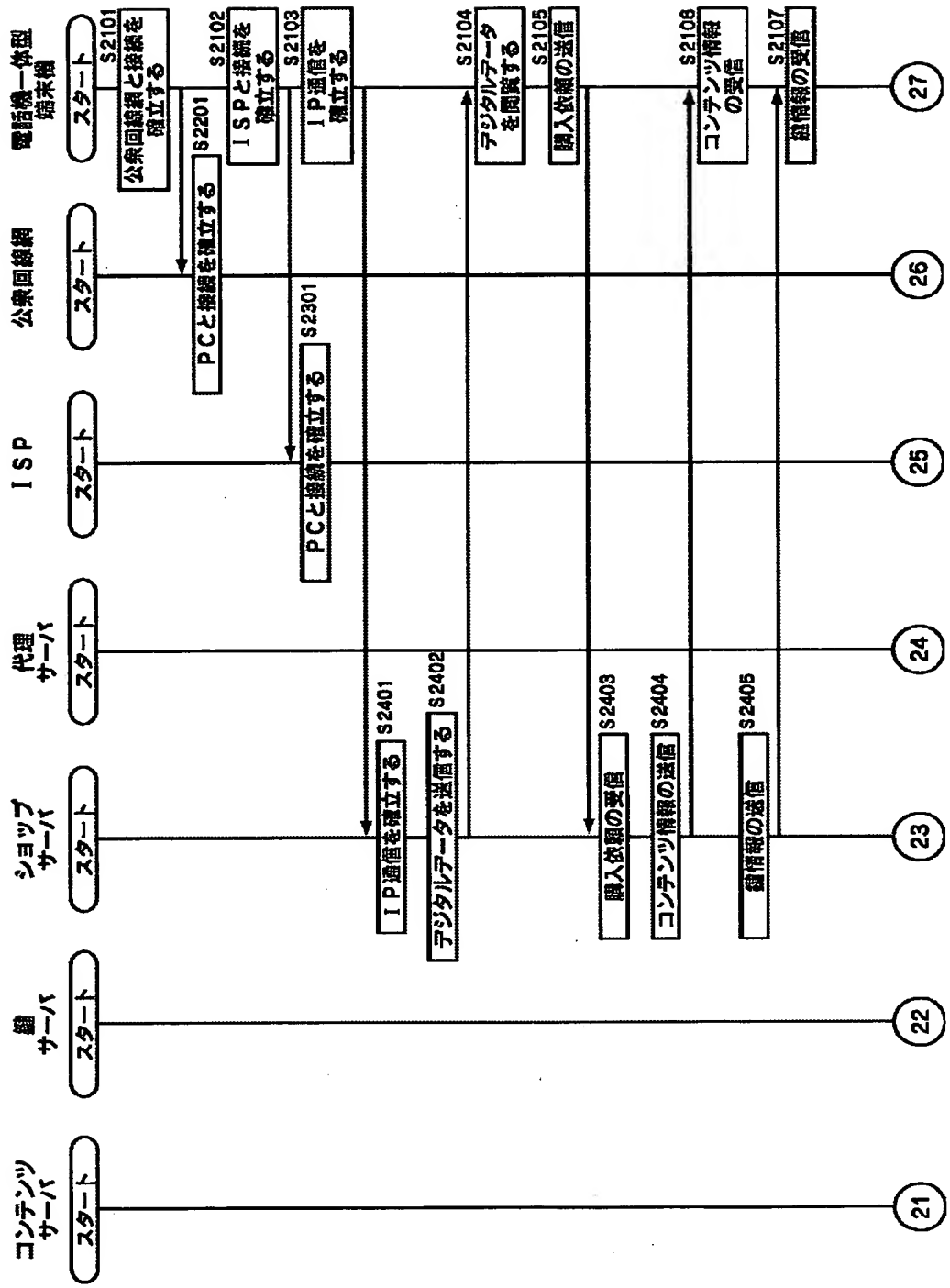
代理サーバ 503

【図１０】


501
電話機一体型端末機
511
表示操作指示プログラム
512
クライアント用ＬＣＭ
711
ライセンス管理プログラム
721
利用条件管理プログラム
722
サーバ認証プログラム
723
ＰＭ認証プログラム
712
ダウンロードプログラム
724
鍵管理プログラム
731
受信プログラム
725
コンテンツ管理プログラム
732
受信プログラム
726
鍵情報受信プログラム
727
コンテンツ情報受信プログラム
713
フォーマット管理プログラム
728
システム識別プログラム
729
フォーマット変換プログラム
701
ＩＰ通信プログラム
741
ＨＴＴＰ
742
Ｗａｐ
702
ＩＳＰ接続プログラム
703
ＰＨＳ／ＩＭＴ通信プログラム
3-1
ＰＭ
101
ライセンス管理プログラム
111
ＰＤ認証プログラム
102
鍵管理プログラム
103
コンテンツ管理プログラム
31
公衆回線網
32
ＩＳＰ
4
通信ネットワーク
23-2
ショップサーバ
21-2
鍵サーバ
22-2
コンテンツサーバ
503
514
代理サーバ
サーバ用ＬＣＭ
781
ライセンス管理プログラム
サーバ認証プログラム
782
ＰＤ認証プログラム
783
シーケンス管理プログラム
鍵管理プログラム
784
鍵受信プログラム
鍵配信プログラム
785
コンテンツ管理プログラム
コンテンツ受信プログラム
786
コンテンツ配信プログラム
システム識別プログラム
751
ＩＰ通信プログラム
787
ＨＴＴＰ
788
Ｗａｐ
23-1
ショップサーバ
121
鍵情報送信プログラム
122
コンテンツ情報送信プログラム
131
鍵管理プログラム
123
検証プログラム
132
検索プログラム
124
ＩＰ通信プログラム
133
ＨＴＴＰ
134
Ｗａｐ
21-1
鍵サーバ
151
鍵認証プログラム
152
鍵配信プログラム
153
鍵保存プログラム
154
鍵生成プログラム
155
ＩＰ通信プログラム
171
ＨＴＴＰ
172
Ｗａｐ
22-1
コンテンツサーバ
191
コンテンツ保存プログラム
192
コンテンツ配信プログラム
193
ＩＰ通信プログラム
201
ＨＴＴＰ
202
Ｗａｐ
761
762
771
772
773

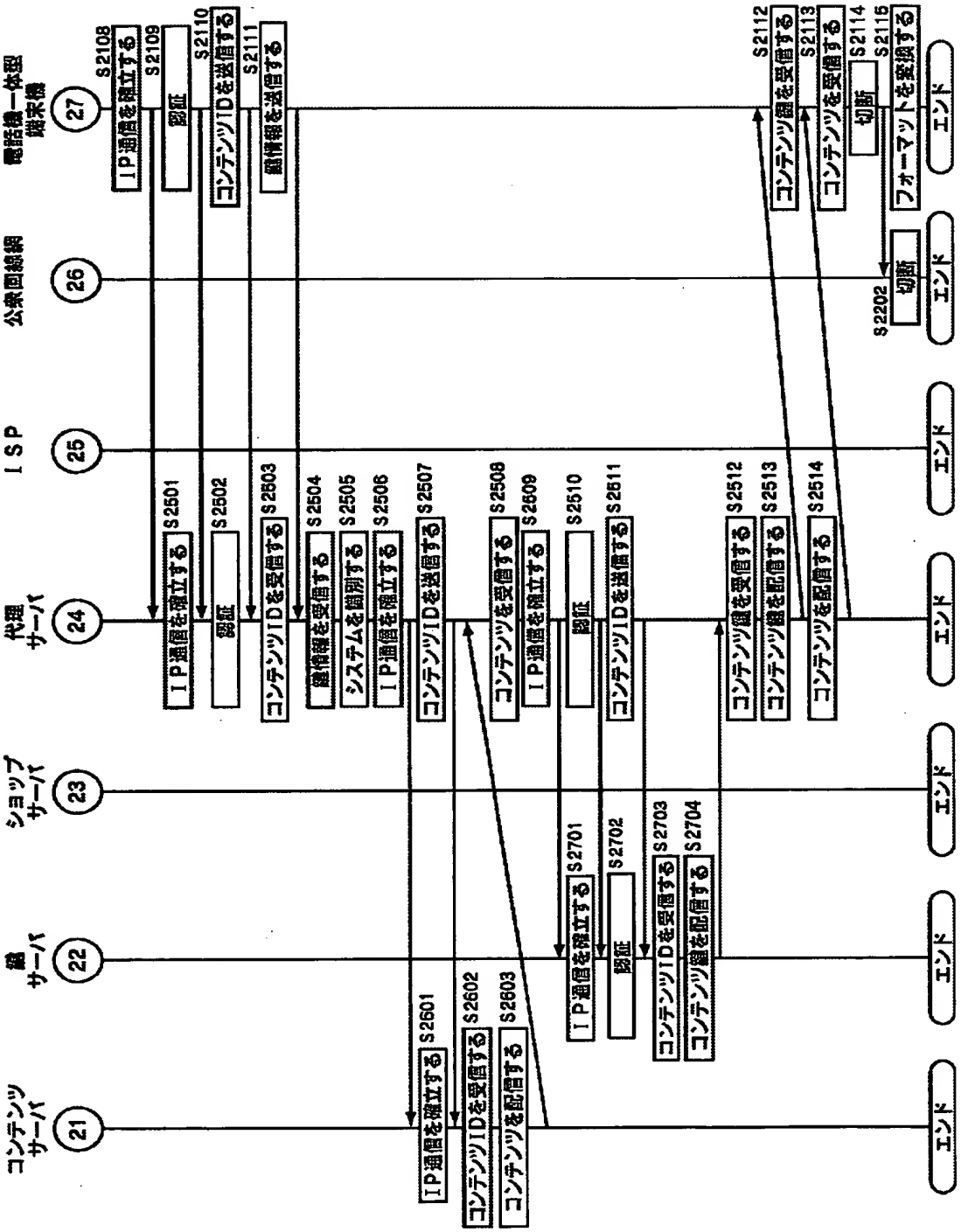
【図１１】

(11－1)


電話機一体型端末機
公衆回線網
ＩＳＰ
代理サーバ
ショップサーバ
銀サーバ
コンテンツサーバ
スタート
S2101
公衆回線網と接続を確立する
S2102
ＩＳＰと接続を確立する
S2103
ＩＰ通信を確立する
S2104
デジタルデータを同期する
S2105
購入依頼の送信
S2106
コンテンツ情報の受信
S2107
個情報の受信
S2201
ＰＣと接続を確立する
S2301
ＰＣと接続を確立する
S2401
ＩＰ通信を確立する
S2402
デジタルデータを送信する
S2403
購入依頼の受信
S2404
コンテンツ情報の送信
S2405
個情報の送信
21
22
23
24
25
26
27

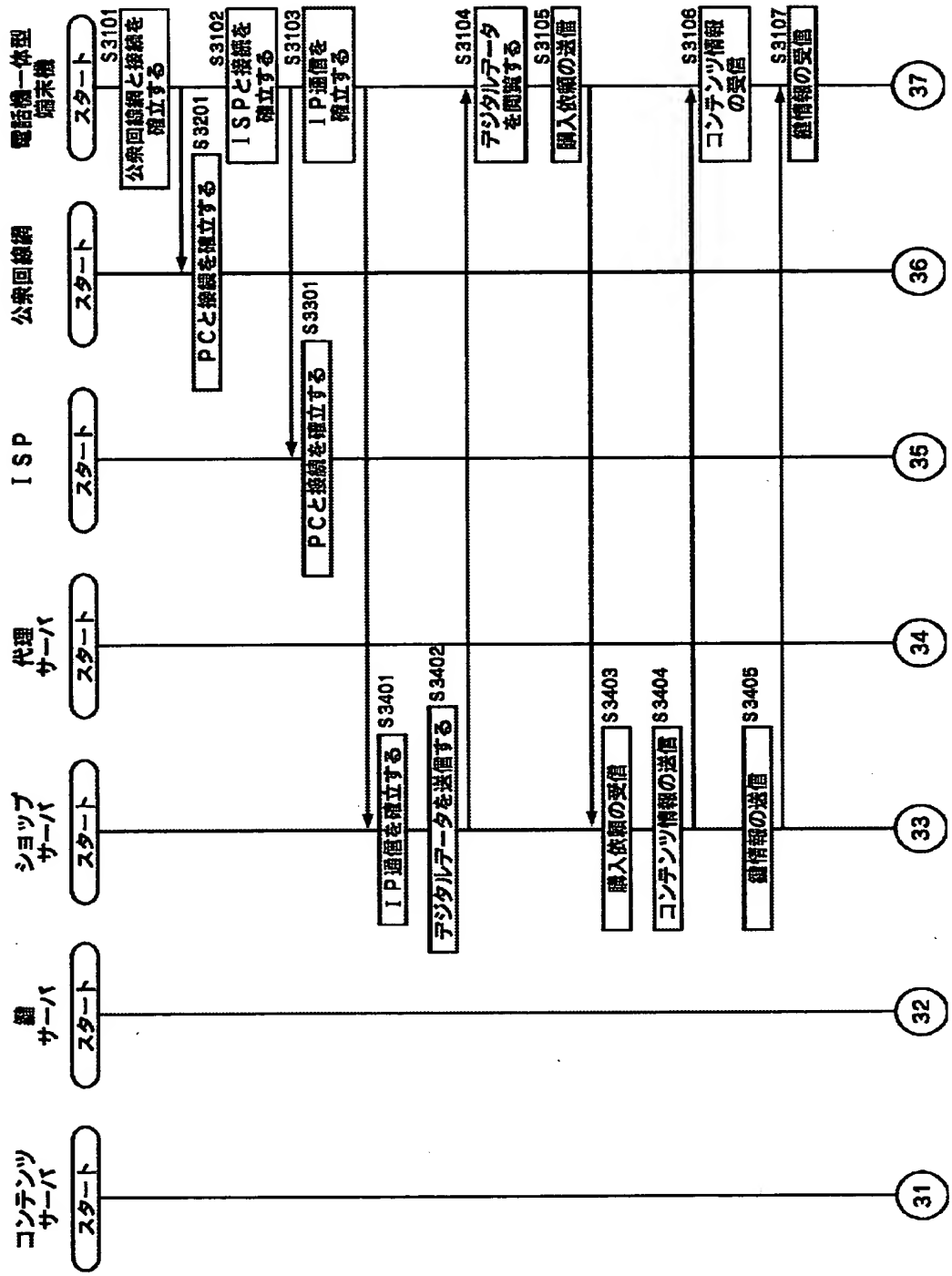
【図１２】

(11－2)


電話機一体型端末機
公衆回線網
ISP
代理サーバ
ショップサーバ
鍵サーバ
コンテンツサーバ
27
26
25
24
23
22
21
S2108 IP通信を確立する
S2109 認証
S2110 コンテンツIDを送信する
S2111 個情報を送信する
S2112 コンテンツ鍵を受信する
S2113 コンテンツを受信する
S2114 切断
S2115 フォーマットを変換する
エンド
S2202 切断
S2501 IP通信を確立する
S2502 認証
S2503 コンテンツIDを受信する
S2504 個情報を受信する
S2505 システムを識別する
S2506 IP通信を確立する
S2507 コンテンツIDを送信する
S2508 コンテンツを受信する
S2609 IP通信を確立する
S2510 認証
S2511 コンテンツIDを送信する
S2512 コンテンツ鍵を受信する
S2513 コンテンツ鍵を配信する
S2514 コンテンツを配信する
S2601 IP通信を確立する
S2602 コンテンツIDを受信する
S2603 コンテンツを配信する
S2701 IP通信を確立する
S2702 認証
S2703 コンテンツIDを受信する
S2704 コンテンツ鍵を配信する

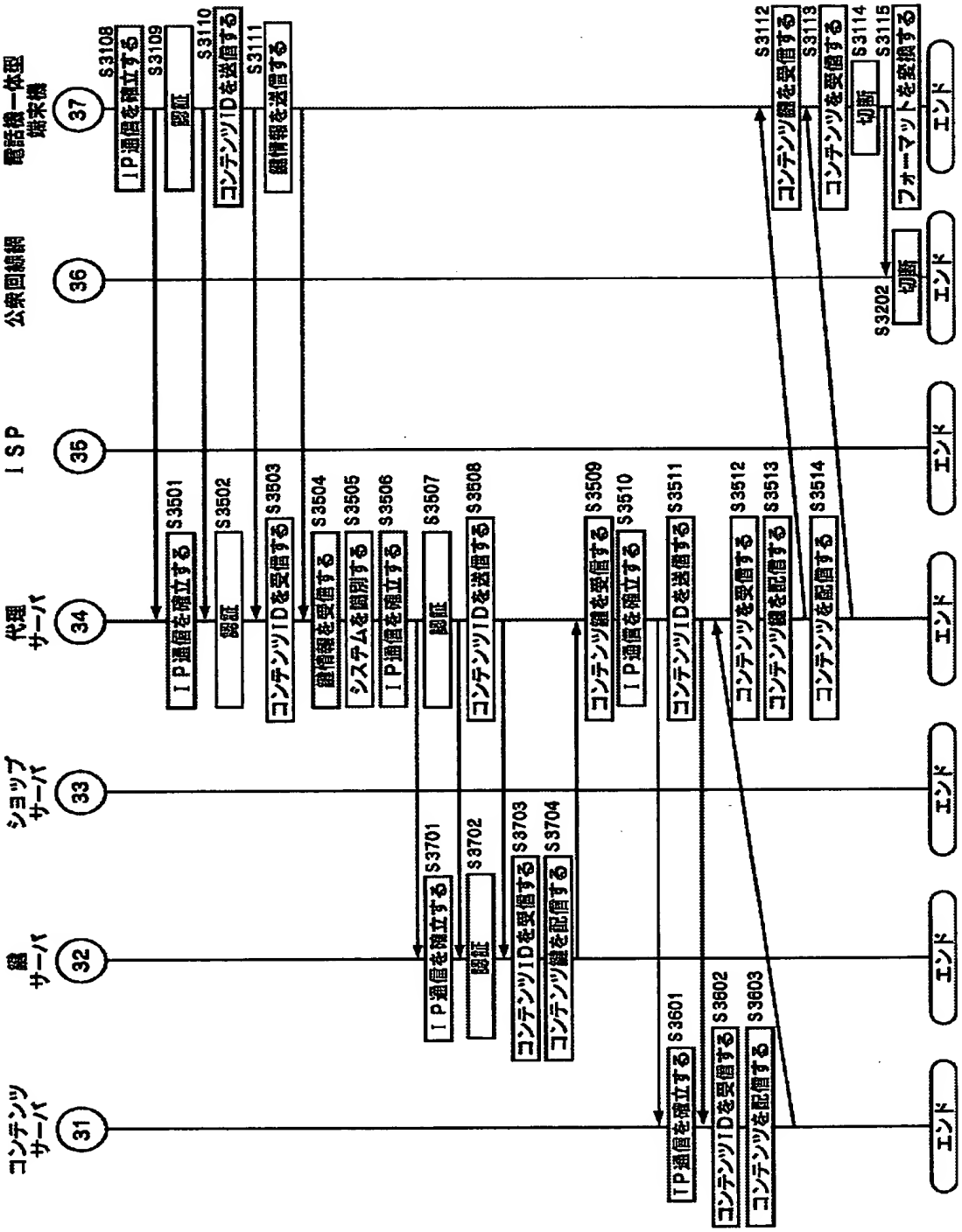
【図１３】

(13－1)

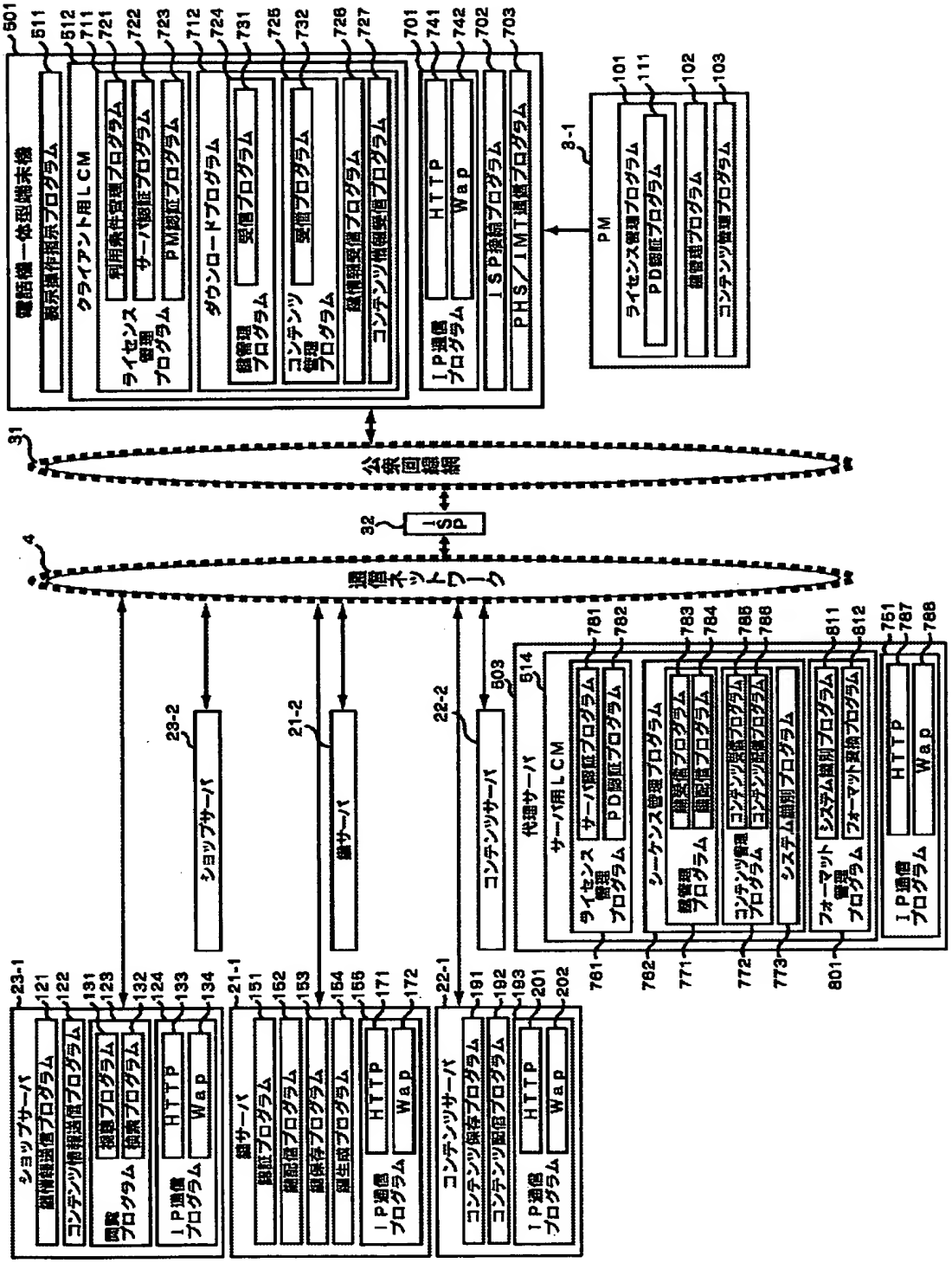

電話機一体型端末機
公衆回線網
ＩＳＰ
代理サーバ
ショップサーバ
鍵サーバ
コンテンツサーバ
スタート
S3101
公衆回線網と接続を確立する
S3102
ＩＳＰと接続を確立する
S3103
ＩＰ通信を確立する
S3104
デジタルデータを同期する
S3105
購入依頼の送信
S3106
コンテンツ情報の受信
S3107
鍵情報の受信
S3201
ＰＣと接続を確立する
S3301
ＰＣと接続を確立する
S3401
ＩＰ通信を確立する
S3402
デジタルデータを送信する
S3403
購入依頼の受信
S3404
コンテンツ情報の送信
S3405
鍵情報の送信
37
36
35
34
33
32
31

【図１４】

(13－2)

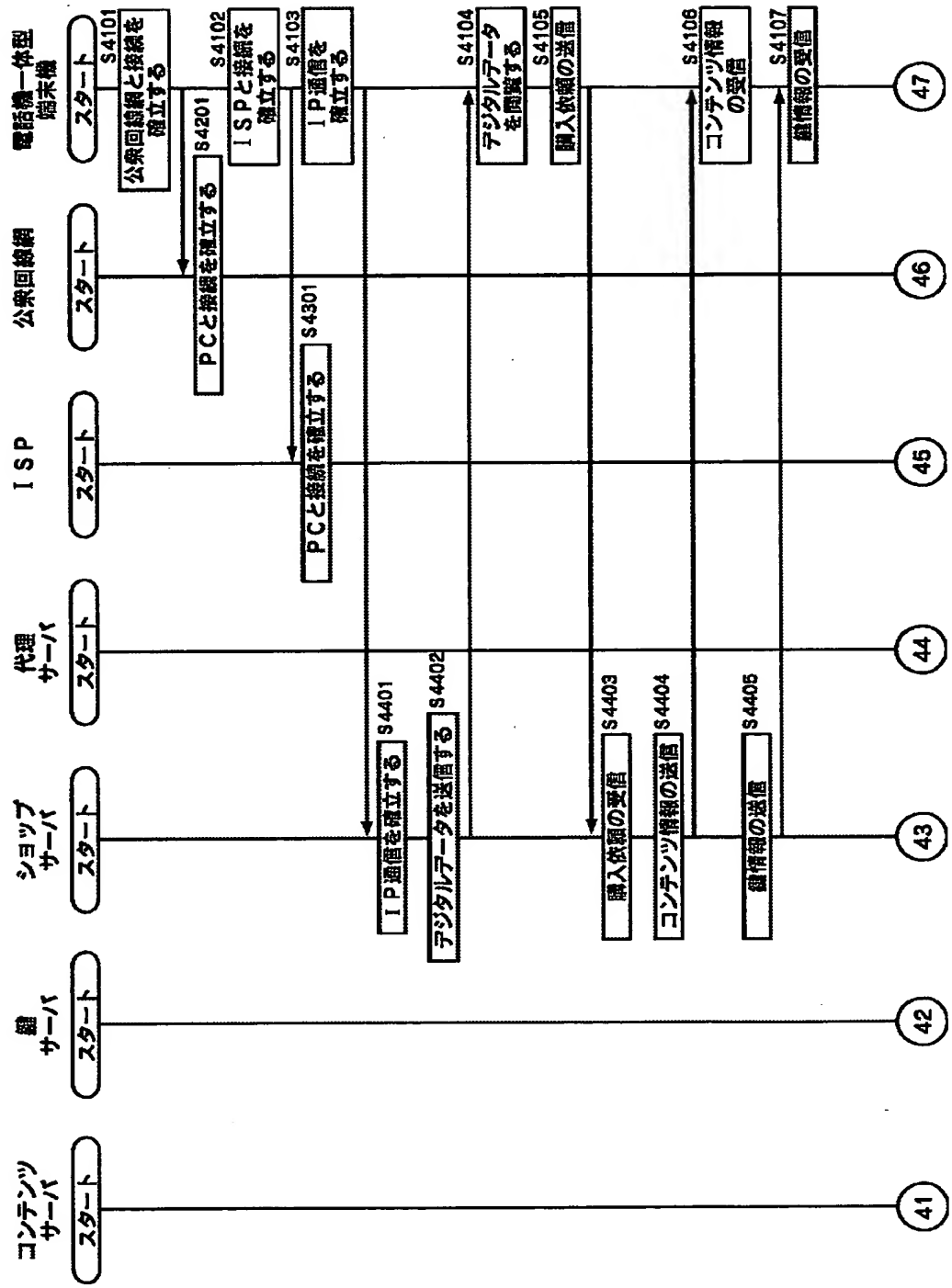

コンテンツサーバ
鍵サーバ
ショップサーバ
代理サーバ
ISP
公衆回線網
電話機一体型端末機
31
32
33
34
35
36
37
エンド
IP通信を確立する
認証
コンテンツIDを送信する
顧情報を送信する
顧情報を受信する
システムを開閉する
コンテンツIDを受信する
コンテンツ鍵を配信する
コンテンツ鍵を受信する
コンテンツを配信する
コンテンツを受信する
切断
フォーマットを変換する
S3101
S3102
S3103
S3104
S3105
S3106
S3107
S3108
S3109
S3110
S3111
S3112
S3113
S3114
S3115
S3201
S3202
S3501
S3502
S3503
S3504
S3505
S3506
S3507
S3508
S3509
S3510
S3511
S3512
S3513
S3514
S3601
S3602
S3603
S3701
S3702
S3703
S3704

【図１５】


501
511
512
711
721
722
723
712
724
731
725
732
726
727
701
741
742
702
703
101
111
102
103
3-1
電話機一体型端末機
表示操作指示プログラム
クライアント用ＬＣＭ
利用条件管理プログラム
サーバ認証プログラム
ＰＭ認証プログラム
ライセンス管理プログラム
ダウンロードプログラム
課金管理プログラム
受信プログラム
コンテンツ管理プログラム
受信プログラム
課情報受信プログラム
コンテンツ情報受信プログラム
ＩＰ通信プログラム
ＨＴＴＰ
Ｗａｐ
ＩＳＰ接続プログラム
ＰＨＳ／ＩＭＴ通信プログラム
ＰＭ
ライセンス管理プログラム
ＰＤ認証プログラム
課管理プログラム
コンテンツ管理プログラム
31
公衆回線網
32
ＩＳＰ
4
通信ネットワーク
23-2
ショップサーバ
21-2
鍵サーバ
22-2
コンテンツサーバ
803
814
代理サーバ
サーバ用ＬＣＭ
ライセンス管理プログラム
サーバ認証プログラム
ＰＤ認証プログラム
781
782
シーケンス管理プログラム
課管理プログラム
課受信プログラム
課配信プログラム
783
784
コンテンツ管理プログラム
コンテンツ受信プログラム
コンテンツ配信プログラム
785
786
システム制御プログラム
811
812
フォーマット管理プログラム
システム制御プログラム
フォーマット変換プログラム
751
787
788
ＩＰ通信プログラム
ＨＴＴＰ
Ｗａｐ
761
782
771
772
773
801
23-1
121
122
131
123
132
124
133
134
ショップサーバ
課情報送信プログラム
コンテンツ情報送信プログラム
課題プログラム
検索プログラム
ＩＰ通信プログラム
ＨＴＴＰ
Ｗａｐ
21-1
151
152
153
154
155
171
172
鍵サーバ
鍵認証プログラム
鍵配信プログラム
鍵保存プログラム
鍵生成プログラム
ＩＰ通信プログラム
ＨＴＴＰ
Ｗａｐ
22-1
191
192
193
201
202
コンテンツサーバ
コンテンツ保存プログラム
コンテンツ配信プログラム
ＩＰ通信プログラム
ＨＴＴＰ
Ｗａｐ

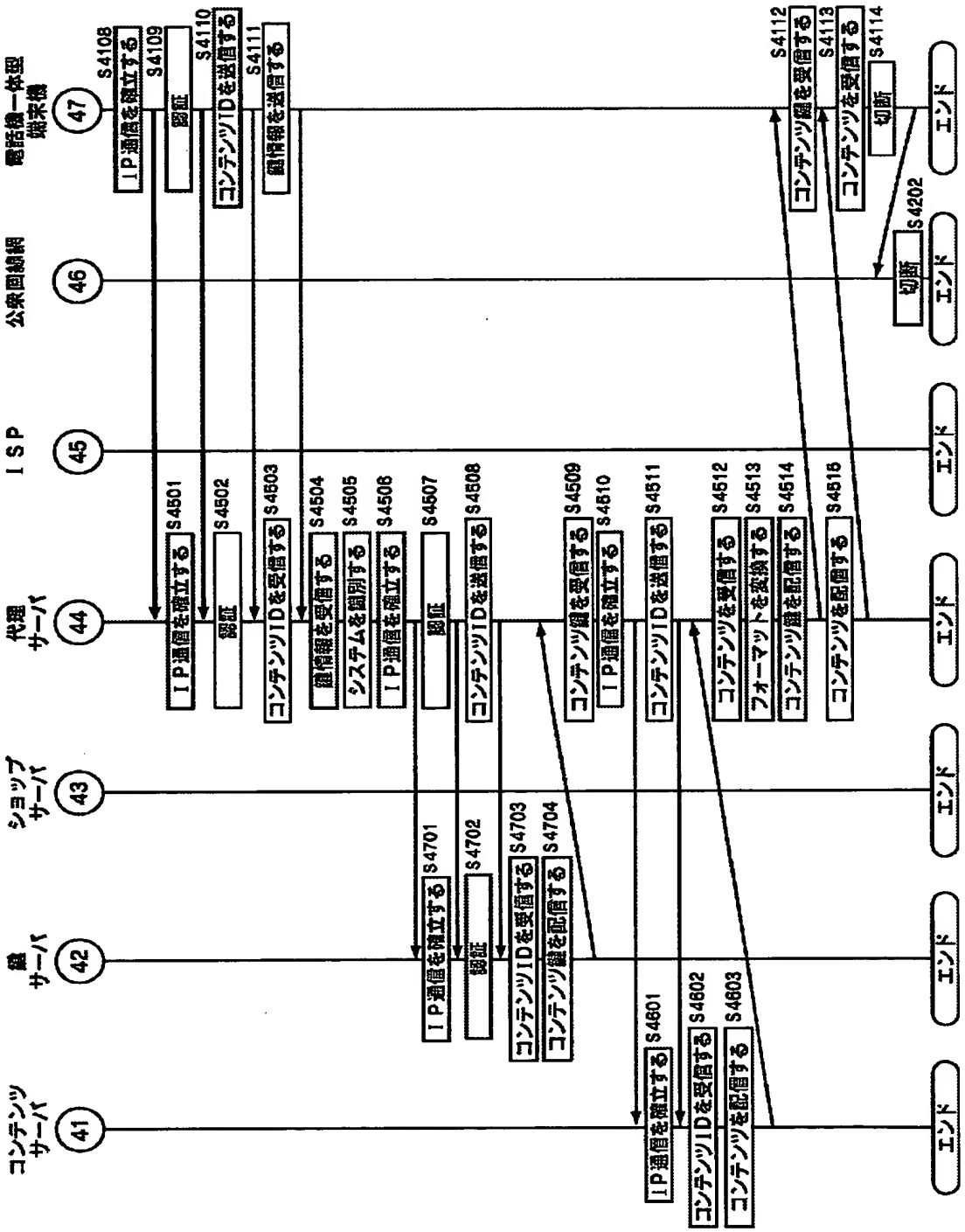
【図１６】

(16−1)


電話機一体型端末機
公衆回線網
ＩＳＰ
代理サーバ
ショップサーバ
銀サーバ
コンテンツサーバ
スタート
S4101
公衆回線網と接続を確立する
S4102
ＩＳＰと接続を確立する
S4103
ＩＰ通信を確立する
S4104
デジタルデータを同覧する
S4105
購入依頼の送信
S4106
コンテンツ情報の受信
S4107
銀情報の受信
S4201
ＰＣと接続を確立する
S4301
ＰＣと接続を確立する
S4401
ＩＰ通信を確立する
S4402
デジタルデータを送信する
S4403
購入依頼の受信
S4404
コンテンツ情報の送信
S4405
銀情報の送信
47
46
45
44
43
42
41

【図１７】

(16−2)


コンテンツサーバ
鍵サーバ
ショップサーバ
代理サーバ
ISP
公衆回線網
電話線一体型端末機
41
42
43
44
45
46
47
S4108
IP通信を確立する
S4109
認証
S4110
コンテンツIDを送信する
S4111
個情報を送信する
S4112
コンテンツ鍵を受信する
S4113
コンテンツを受信する
S4114
切断
S4202
切断
エンド
S4501
IP通信を確立する
S4502
認証
S4503
コンテンツIDを受信する
S4504
個情報を受信する
S4505
システムを個別する
S4506
IP通信を確立する
S4507
認証
S4508
コンテンツIDを送信する
S4509
コンテンツ鍵を受信する
S4510
IP通信を確立する
S4511
コンテンツIDを送信する
S4512
コンテンツを受信する
S4513
フォーマットを変換する
S4514
コンテンツ鍵を配信する
S4515
コンテンツを配信する
S4701
IP通信を確立する
S4702
認証
S4703
コンテンツIDを受信する
S4704
コンテンツ鍵を配信する
S4601
IP通信を確立する
S4602
コンテンツIDを受信する
S4603
コンテンツを配信する

【書類名】　　要約書

【要約】

【課題】　異なる手順で供給されるコンテンツおよび鍵を受信する。

【解決手段】　ライセンス管理プログラム７６１は、電話機一体型端末機５０１を認証するとともに、第１のサーバまたは第２のサーバを認証する。サーバ用ＬＣＭ５１４は、コンテンツおよび鍵の送信要求、並びに第１のサーバを特定するデータまたは第２のサーバを特定するデータの受信を制御して、第１のサーバを特定するデータを受信した場合、第１のサーバに対応する手続で、第１のサーバからコンテンツおよび鍵を受信し、第２のサーバを特定するデータを受信した場合、第２のサーバに対応する手続で、第２のサーバからコンテンツおよび鍵を受信するように通信を制御する。サーバ用ＬＣＭ５１４は、電話機一体型端末機５０１へのコンテンツおよび鍵の送信を制御する。

【選択図】　　図１０

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社